An introduction to algorithmic randomness

Fourth Workshop on Game-Theoretic Probability and Related Topics
12 -14 Nov 2012 The University of Tokyo

Kenshi Miyabe
Research Institute for Mathematical Sciences,
Kyoto University

Overview

- Defining randomness notions - three approaches
- Each random sequence has a property
- Existence of a random sequence with a propery
- Partial randomness
- Historical comment

Definitions of random sequences

FAIR-COIN GAME

Players: Skeptic, Reality

Protocol:

$\mathcal{K}_0 := 1.$

FOR $n = 1, 2, \ldots$:

Skeptic announces $M_n \in \mathbb{R}$.

Reality announces $x_n \in \{0, 1\}$.

$\mathcal{K}_n := \mathcal{K}_{n-1} + M_n(x_n - \frac{1}{2})$.

Collateral Duties: Skeptic must keep $\mathcal{K}_n$ non-negative. Reality must keep $\mathcal{K}_n$ from tending to infinity.

An interpretation

1. In the fair coin protocol, $\limsup_n \mathcal{K}_n < \infty$ almost surely.
2. Consider the realized sequence $\{x_n\}$.
3. $\{x_n\}$ is "random" with respect to Skeptic.
4. Fix a strategy of Skeptic.
5. Then $\{x_n\}$ is "random" with respect to the strategy.

How to describe a strategy

Let $\sigma \in 2^*$.

We write $d(\sigma)$ to mean $\mathcal{K}_{|\sigma|}$ when $\{x_n\} = \{\sigma(1), \sigma(2), \cdots\}$.

Then

$$\begin{aligned} d(\sigma 0) + d(\sigma 1) =& \mathcal{K}_{|\sigma|} + M_{|\sigma|}(0 - \frac{1}{2}) + \mathcal{K}_{|\sigma|} + M_{|\sigma|}(1 - \frac{1}{2}) \\ =& 2\mathcal{K}_{|\sigma|} = 2d(\sigma). \end{aligned}$$

Thus all strategies should have this average property.

Conversely, one can calculate M_n from d.

Martingales in randomness

Definition

A martingale is a function $d : 2^* \to \mathbb{R}^+$ such that

$$2d(\sigma) = d(\sigma 0) + d(\sigma 1).$$

A martingale is a capital process but we think this is also describing a betting strategy.

A sequence $A \in 2^\omega$ is "random" for a martingale d if

$$\limsup_n d(A \upharpoonright n) < \infty.$$

Random for a class

No sequence is "random" for every martingale d.

So consider a countable class $\mathcal{C}$ of martingales.

Definition

Let $\mathcal{C}$ be a countable class of martingales.

Let us call a sequence A $\mathcal{C}$-random if

$$\limsup_{n} d(A \upharpoonright n) < \infty$$

for all $d \in \mathcal{C}$.

Computability is the essence

One natural class is the class of computable martingales.

A function $f : 2^* \to 2^*$ is computable if it is computable by a Turing machine.

The computability of functions $f : \mathbb{N} \to \mathbb{N}$ and $g : \mathbb{N} \to \mathbb{Q}$ are induced from the above.

A real α is computable if there is a computable sequence $\{p_n\}$ of rationals such that $|\alpha - p_n| \leq 2^{-n}$ for all n.

The computability of a function $d : 2^* \to \mathbb{R}^+$ is defined similarly.

Computable randomness

Definition (Schnorr 1971)

A sequence $A \in 2^*$ is called computably random if

$$\limsup_n d(A \restriction n) < \infty$$

for all computable martingales d. .

ML-randomness

A real α is c.e. if there is an increasing computable sequence $\{p_n\}$ of rationals such that $\alpha = \lim_n p_n$.

The notion of c.e. for a function $d : 2^* \to \mathbb{R}^+$ is defined similarly.

Theorem (Schnorr 1971)

A sequence $A \in 2^\omega$ is Martin-Löf random iff

$$\limsup_n d(A \upharpoonright n) < \infty$$

for all c.e. martingales d. .

Hierarchy of randomness notions

Martin-Löf randomness

$\rotatebox{90}{$\supsetneq$}$

computable randomness

$\rotatebox{90}{$\supsetneq$}$

Schnorr randomness

$\rotatebox{90}{$\supsetneq$}$

Kurtz randomness

ML-tests

Consider Cantor space 2^ω with the uniform measure μ.

Definition (Martin-Löf 1966)

A ML-test is a sequence $\{U_n\}$ of uniformly c.e. open sets with $\mu(U_n) \leq 2^{-n}$.

A sequence $A \in 2^\omega$ is ML-random if $A \notin \bigcap_n U_n$ for all ML-tests.

Complexity

Definition

Fix a prefix-free universal Turing machine U.

For a string $\sigma \in 2^*$, we define $K(\sigma)$ by

$$K(\sigma) = \min\{|\tau| \ : \ U(\tau) = \sigma\}.$$

Theorem (Levin, Schnorr, Chaitin)

A is ML-random iff there exists c such that

$$K(A \upharpoonright n) > n - c$$

for all n.

Three (big) approaches

- Typicalness - tests
- Unpredictability - martingales
- Incompressibility - complexity

Technical similarity

Their purposes are different

- Game-theoretic probability
  - Which event has probability 0 or 1?
  - To explain a phenomenon.
- Algorithmic randomness
  - What does it mean by saying that an individual sequence is random?

Skeptic can force an event.

Skeptic can force an event E.

$\Rightarrow$ If Skeptic use a strategy, then $\{x_n\} \in E$ unless $\mathcal{K}_n \to \infty$.

$\Rightarrow$ If $\{x_n\}$ is "random" with respect to the strategy,

then $\{x_n\} \in E$.

- E has probability 1.
- Skeptic can force an event E.
- A random sequence has the property E.

Strong law of large numbers

Theorem (SLLN)

Let $\{X_n\}$ be the sequence of i.i.d. random variables such that $P(X_1 = 0) = P(X_1 = 1) = 1/2$. Then $S_n/n \to 1/2$ almost surely.

Theorem

In the fair-coin game, Skeptic can force $S_n/n \to 1/2$.

Theorem

Let A be a ML-random sequence. Then $S_n(A)/n \to 1/2$.

Which randomness is needed?

- Skeptic can force SLLN in a protocol,
but not in another protocol.
- SLLN holds for ML-randomness, computable randomness and Schnorr randomness,
but not for Kurtz randomness.

Reality can comply with an event.

Reality can comply with an event E.

$\Rightarrow$ Irrespective of the move of Skeptic,

$$\{x_n\} \in E \text{ and } \sup_n \mathcal{K}_n < \infty.$$

$\Rightarrow$ There exists a "random" sequence with the property E.

- Reality can comply with an event E.
- There exists a "random" sequence with the property E.

A sequence with a property

In most protocols, Reality can comply

$$\sup_n \mathcal{K}_n \leq \mathcal{K}_0.$$

Notice that Reality has a deterministic strategy.

For each computable martingale d, there exists a computable sequence A such that

$$\sup_n d(A \upharpoonright n) \leq d(\lambda) + 1.$$

How random is a sequence?

Let A be a ML-random sequence.

Then $A \oplus \emptyset$ is *1/2-random.*

Definition

Let $s \in [0, 1]$.

A is called weakly s-random if $\exists d \forall n K(A \upharpoonright n) \geq sn - d$.

How fast does the capital increase?

Definition

For a martingale d and an order h, the h-success set of d is

$$S_h[d] = \{A \ : \ \limsup_n \frac{d(A \upharpoonright n)}{h(n)} = \infty\}.$$

Theorem

Let $s \in [0, 1]$. If A is weakly s-random, then $A \notin S_{2^{(1-t)n}}[d]$ for all c.e. supermartingales d and all $t < s$.

Other topics

- Many measures of randomness
- Less or more random
- The relation with computability
- Randomness in a general space

Historical comment

What is probability?

- von Mises - “First collective, then probability”
- Martin-Löf, Schnorr, Levin, Kolmogorov
  - typicality, unpredictability, incompressibility
- Solomonoff
  - algorithmic probability, universal prior
- game-theoretic probability, defensive forecasting

Two approaches

- Axiomatic approach (or Hilbert's approach)
  - probability => randomness
- Our approach
  - randomness => probability