

# Probability, Randomness, Entropy

## Convenience or Necessity?

C. S. Calude  
University of Auckland  
`www.cs.auckland.ac.nz/~cristian`

*Débat sur la phase actuelle du concept de probabilité et d'aléatoire*  
École Normale Supérieure, Paris, October 2011

## Probability as attitude of mind

The proposition of interest: “Will a specific event occur?” .

The attitude of mind: “How certain are we that the event will occur?” .

Probability can be used to describe the mind’s attitude towards the proposition whose truth we are not certain [?].

The higher the probability of an event, the more certain we are that the event will occur.

## Applying probability

In an applied sense, probability is a measure of the likeliness that a **random** event will occur.

This raises the question: “What is a random event”?

Kolmogorov’s axiomatics ignores this question: instead, it proposes a calculus with unspecified “random events”.

# Randomness

Using a cocktail of computability theory, probability theory and Shannon's information theory, algorithmic information theory [?] defines/studies various "algorithmic random objects".

The set of Martin-Löf algorithmic random reals is a model of "random events" for Lebesgue's probability.

"True randomness" does not exist from a mathematical point of view.

# Entropy

Shannon's entropy is a measure of the average information content one is missing when one does not know the value of the random variable.

There are many notions of “entropy”. All seem to be intrinsically random-based...

Algorithmically coding theorem [?]: Shannon's entropy is up to an additive constant equal to prefix complexity, a pure deterministic concept.

## Probability as convenience

By interpreting some events as “random” we can solve problems:

- ▶ efficiently testing primality (theoretically easy, practically hard)
- ▶ solving the halting problem (algorithmically unsolvable).





## Probability as necessity

Quantum mechanics seems to require probability.

Under some natural assumptions, 'quantum randomness' can be proved to be strongly incomputable [?].

Our paper [?] describes a quantum random generator which produces "incomputable quantum random bits".

Suggestion: there are different forms of 'quantum randomness'.

-  A. Abbott, C. S. Calude, K. Svozil. A quantum random number generator certified by value indefiniteness, *Mathematical Structures in Computer Science* (2012), to appear.
-  C. S. Calude. *Information and Randomness: An Algorithmic Perspective*, Springer-Verlag, Berlin, 2002 (2nd edition).
-  C. S. Calude, K. Svozil. Quantum randomness and value indefiniteness, *Advanced Science Letters*, 1:165–168, 2008.
-  A. Stuart, K. Ord. *Kendall's Advanced Theory of Statistics*, Volume 1: Distribution Theory, Wiley, Hoboken, NJ 2009 (6th edition).