Randomness: Where Is It Coming From and How Random Is It?

Cristian S. Calude
University of Auckland

TU Vienna, June 2011

The intuition of randomness

- **Unpredictability:** It is impossible to win against a random sequence in a fair betting game.

The intuition of randomness

- **Unpredictability:** It is impossible to win against a random sequence in a fair betting game.
- **Incompressibility:** It is impossible to compress a random sequence.

The intuition of randomness

- **Unpredictability:** It is impossible to win against a random sequence in a fair betting game.
- **Incompressibility:** It is impossible to compress a random sequence.
- **Typicalness:** Random sequences pass every statistical test of randomness.

Kolmogorov axiomatic probability theory assigns probabilities to sets of outcomes and shows how to calculate with such probabilities: **it assumes randomness, but does not distinguish between individual random and non-random elements**.

Kolmogorov axiomatic probability theory assigns probabilities to sets of outcomes and shows how to calculate with such probabilities: **it assumes randomness, but does not distinguish between individual random and non-random elements**.

For example, under a uniform distribution, the outcome of n zeros

$$000000000000000 \cdots 0$$

has the same probability as any other outcome of length n, namely 2^{-n}.

The math of randomness: probability theory

00000000000000000000000000000000

The math of randomness: probability theory

00000000000000000000000000000000

10011001100110011001100110011001

The math of randomness: probability theory

00000000000000000000000000000000

10011001100110011001100110011001

10011001100110010110011001100110

The math of randomness: probability theory

00000000000000000000000000000000

10011001100110011001100110011001

10011001100110010110011001100110

01000110110000010100111001011101

The math of randomness: probability theory

00000000000000000000000000000000

10011001100110011001100110011001

10011001100110010110011001100110

01000110110000010100111001011101

0100011001000001010000100101001

The math of randomness: probability theory

00000000000000000000000000000000

10011001100110011001100110011001

10011001100110010110011001100110

01000110110000010100111001011101

0100011001000001010000100101001

10011111010001110001100001101101

The math of randomness: no definition of “randomness”

No mathematical definition of “randomness” can satisfy all intuitive features of randomness, in particular, unpredictability, incompressibility, typicalness.

The math of randomness: no definition of “randomness”

No mathematical definition of “randomness” can satisfy all intuitive features of randomness, in particular, unpredictability, incompressibility, typicalness.

Specifically, **there is no infinite sequence passing all tests of randomness.**

The math of randomness: no definition of “randomness”

Ramsey theory (named after the British mathematician and philosopher Frank P. Ramsey) is a branch of mathematics that studies the conditions under which order must appear.

Ramsey theory (named after the British mathematician and philosopher Frank P. Ramsey) is a branch of mathematics that studies the conditions under which order must appear.

Van der Waerden Theorem: *In every binary sequence at least one of the two symbols must occur in arithmetical progressions of every length.*

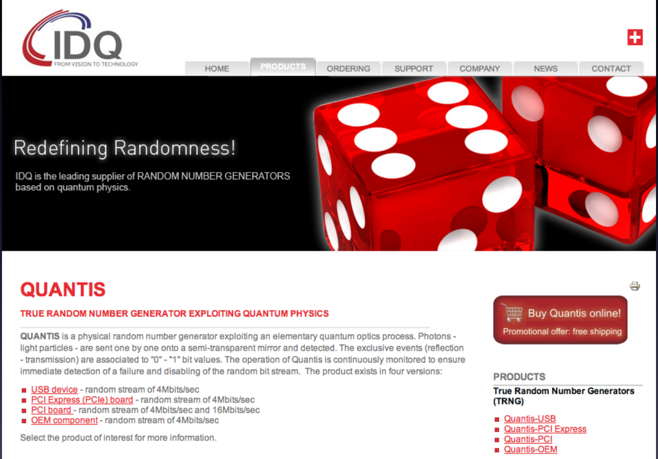
In spite of mathematical evidence, generators of true random bits proliferate.

True randomness?

Nature (doi:10.1038/news.2010.181, 14 April 2010):

Truly random numbers have been generated at last.

True randomness?



Study this paragraph and all things in it. What is vitally distinct about it? Actually, nothing is wrong, but you must admit that it is most unusual. Don't just zip through it quickly but study it scrupulously. With a bit of luck you should spot what it is so particular about it and all words found in it. Can you say what it is? Try hard as isn't it all that difficult.

AIT uses computability theory to model “finite (algorithmic) random strings” and “infinite (algorithmic) random sequences”.

- Defining strings with Turing machines: $T(d) = x$.

The math of randomness: finite (algorithmic) random strings

- Defining strings with Turing machines: $T(d) = x$.
- Compressing strings: if $T(d) = x$ and $|d| < |x|$, then x is not algorithmic random.

The math of randomness: finite (algorithmic) random strings

- Defining strings with Turing machines: $T(d) = x$.
- Compressing strings: if $T(d) = x$ and $|d| < |x|$, then x is not algorithmic random.
- Definition of algorithmic random strings: a string x is Kolmogorov/Chaitin random if there are no T and d such that $T(d) = x$ and $|d| < |x|$.

- Defining strings with Turing machines: $T(d) = x$.
- Compressing strings: if $T(d) = x$ and $|d| < |x|$, then x is not algorithmic random.
- Definition of algorithmic random strings: a string x is Kolmogorov/Chaitin random if there are no T and d such that $T(d) = x$ and $|d| < |x|$.
- Kolmogorov/Chaitin random strings of every length exist (and abound).

- Defining strings with Turing machines: $T(d) = x$.
- Compressing strings: if $T(d) = x$ and $|d| < |x|$, then x is not algorithmic random.
- Definition of algorithmic random strings: a string x is Kolmogorov/Chaitin random if there are no T and d such that $T(d) = x$ and $|d| < |x|$.
- Kolmogorov/Chaitin random strings of every length exist (and abound).
- There is no algorithm deciding whether a string is Kolmogorov/Chaitin random.

The math of randomness: finite (algorithmic) random strings

- Defining strings with Turing machines: $T(d) = x$.
- Compressing strings: if $T(d) = x$ and $|d| < |x|$, then x is not algorithmic random.
- Definition of algorithmic random strings: a string x is Kolmogorov/Chaitin random if there are no T and d such that $T(d) = x$ and $|d| < |x|$.
- Kolmogorov/Chaitin random strings of every length exist (and abound).
- There is no algorithm deciding whether a string is Kolmogorov/Chaitin random.
- Kolmogorov/Chaitin random strings cannot be enumerated by a Turing machine.

- An infinite sequence is Kolmogorov/Chaitin random if its prefixes are “almost” Kolmogorov/Chaitin random.

- An infinite sequence is Kolmogorov/Chaitin random if its prefixes are "almost" Kolmogorov/Chaitin random.
- Kolmogorov/Chaitin random infinite sequences pass all computably enumerable tests of randomness. For example, they pass the test of normality.

The math of randomness: infinite (algorithmic) random sequences

- An infinite sequence is Kolmogorov/Chaitin random if its prefixes are “almost” Kolmogorov/Chaitin random.
- Kolmogorov/Chaitin random infinite sequences pass all computably enumerable tests of randomness. For example, they pass the test of normality.
- Every Kolmogorov/Chaitin random infinite sequence is incomputable.

- An infinite sequence is Kolmogorov/Chaitin random if its prefixes are “almost” Kolmogorov/Chaitin random.
- Kolmogorov/Chaitin random infinite sequences pass all computably enumerable tests of randomness. For example, they pass the test of normality.
- Every Kolmogorov/Chaitin random infinite sequence is incomputable.
- With probability one every infinite sequence is Kolmogorov/Chaitin random.

(i) Pseudo-randomness produced by software like *Mathematica* or *Maple*: not only Turing computable but cyclic.

(i) Pseudo-randomness produced by software like *Mathematica* or *Maple*: not only Turing computable but cyclic.

(ii) Turing computable but not cyclic pseudo-randomness (digits of π or Champernowne's constant).

Degrees of randomness

(i) Pseudo-randomness produced by software like *Mathematica* or *Maple*: not only Turing computable but cyclic.

(ii) Turing computable but not cyclic pseudo-randomness (digits of π or Champernowne's constant).

(iii) Turing incomputable, but not Kolmogorov/Chaitin random.

(i) Pseudo-randomness produced by software like *Mathematica* or *Maple*: not only Turing computable but cyclic.

(ii) Turing computable but not cyclic pseudo-randomness (digits of π or Champernowne's constant).

(iii) Turing incomputable, but not Kolmogorov/Chaitin random.

(iv) Kolmogorov/Chaitin random.

Degrees of randomness

(i) Pseudo-randomness produced by software like *Mathematica* or *Maple*: not only Turing computable but cyclic.

(ii) Turing computable but not cyclic pseudo-randomness (digits of π or Champernowne's constant).

(iii) Turing incomputable, but not Kolmogorov/Chaitin random.

(iv) Kolmogorov/Chaitin random.

In which of these four classes do we find quantum randomness?

Born's 1926 decision to "give up determinism in the world of atoms" has become a core part of our understanding of quantum mechanics.

No-go theorems (such as the Kochen-Specker theorem ▸ NGT) are stronger: if we assume non-contextuality, then there can, in general, be no pre-existing definite values (value indefiniteness) prescribable to certain sets of measurement outcomes in dimension three or greater Hilbert space.

Assume

Assume

- a standard picture of quantum mechanics, i.e. a Copenhagen-like interpretation in which measurement produces a result and irreversibly alters the quantum state,

Quantum randomness incomputability

Assume

- a standard picture of quantum mechanics, i.e. a Copenhagen-like interpretation in which measurement produces a result and irreversibly alters the quantum state,
- measurements are non-contextual,

Quantum randomness incomputability

Assume

- a standard picture of quantum mechanics, i.e. a Copenhagen-like interpretation in which measurement produces a result and irreversibly alters the quantum state,
- measurements are non-contextual,
- and the experimenter has freedom in the choice of measurement basis (the “free-will assumption").

Under the above assumptions, a quantum random experiment certified by value indefiniteness and performed under ideal conditions generates an infinite (strongly) incomputable sequence of bits:

> *every Turing machine can reproduce exactly only finitely many scattered digits of such an infinite sequence, i.e. the sequence is bi-immune.*

Experimental evidence for quantum randomness incomputability

Data consisting of 2^{32}–bit strings:

Data consisting of 2^{32}–bit strings:

1. 10 quantum random strings generated by the *Vienna IQOQI* group

Experimental evidence for quantum randomness incomputability

Data consisting of 2^{32}–bit strings:

1. 10 quantum random strings generated by the *Vienna IQOQI* group
2. 10 quantum random strings generated with the *Quantis* device

Experimental evidence for quantum randomness incomputability

Data consisting of 2^{32}–bit strings:

1. 10 quantum random strings generated by the *Vienna IQOQI* group
2. 10 quantum random strings generated with the *Quantis* device
3. 10 strings from the binary expansion of π obtained from the University of Tokyo's supercomputing center

Data consisting of 2^{32}–bit strings:

1. 10 quantum random strings generated by the *Vienna IQOQI* group
2. 10 quantum random strings generated with the *Quantis* device
3. 10 strings from the binary expansion of π obtained from the University of Tokyo's supercomputing center
4. 10 pseudo-random strings produced by *Mathematica* 6

Experimental evidence for quantum randomness incomputability

Data consisting of 2^{32}–bit strings:

1. 10 quantum random strings generated by the *Vienna IQOQI* group
2. 10 quantum random strings generated with the *Quantis* device
3. 10 strings from the binary expansion of π obtained from the University of Tokyo's supercomputing center
4. 10 pseudo-random strings produced by *Mathematica* 6
5. 10 pseudo-random strings produced by *Maple* 11

For any fixed integer $m > 1$, $B_m = \{0, 1\}^m$, and for every $1 \leq i \leq 2^m$ denote by N_i^m the number of occurrences of the lexicographical ith binary string of length m in the string x over B_m. By $|x|_m$ we denote the length of x

Normality test

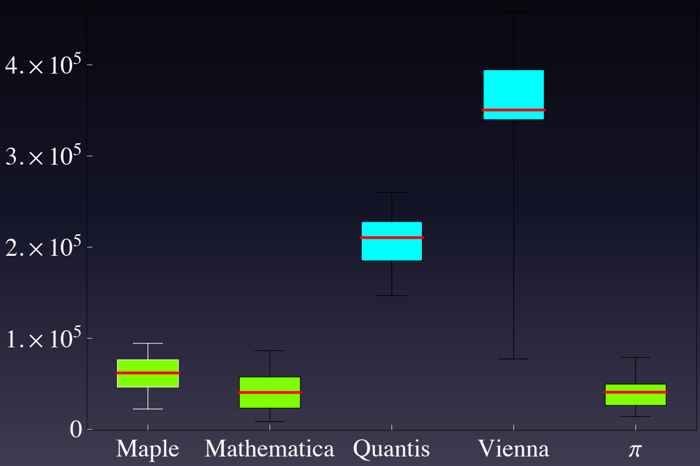
For any fixed integer $m > 1$, $B_m = \{0,1\}^m$, and for every $1 \le i \le 2^m$ denote by N_i^m the number of occurrences of the lexicographical ith binary string of length m in the string x over B_m. By $|x|_m$ we denote the length of x

A string x is normal if for every natural $1 \le m \le \log_2 \log_2 |x|$,

$$\left| \frac{N_j^m(x)}{|x|_m} - 2^{-m} \right| \le \sqrt{\frac{\log_2 |x|}{|x|}},$$

for every $1 \le j \le 2^m$.

Box-and-whisker plot



Statistical significance

Table: Kolmogorov-Smirnov test for normality tests.

Kolmogorov-Smirnov test p-values	Mathematica	Quantis	Vienna	π
Maple	0.4175	$< 10^{-4}$	**0.0002**	0.1678
Mathematica		$< 10^{-4}$	**0.0002**	0.9945
Quantis			**0.0002**	$< 10^{-4}$
Vienna				**0.0002**

References

A. A. Abbott, C. S. Calude. Von Neumann Normalisation of a Quantum Random Number Generator, *CDMTCS Research Report* 392, 2010, 26 pp.

A. A. Abbott, C. S. Calude, K. Svozil. Incomputability of quantum randomness, in preparation, 2011.

C. S. Calude, M. J. Dinneen, A. M. Gardner. Opening the Book of Randomness (Extended Version), *CDMTCS Research Report* 393, 2010, 19 pp.

C. S. Calude, K. Svozil. Quantum randomness and value indefiniteness, *Advanced Science Letters* 1 (2008), 165–168.

C. S. Calude, M. J. Dinneen, M. Dumitrescu, K. Svozil. Experimental evidence of quantum randomness incomputability, *Physical Review A*, 82, 022102 (2010), 1–8.

No-go theorem

A no-go theorem is a theorem that states that a particular situation is not physically possible.

A no-go theorem is a theorem that states that a particular situation is not physically possible.

Bell's theorem: No physical theory of local hidden variables can reproduce all QM predictions.

Kochen-Specker theorem

In QM, VD + NC is contradictory:

VD: All observables defined for a QM system have definite values at all times.

NC: If a QM system possesses a property (value of an observable), then it does so independently of how that value is eventually measured.

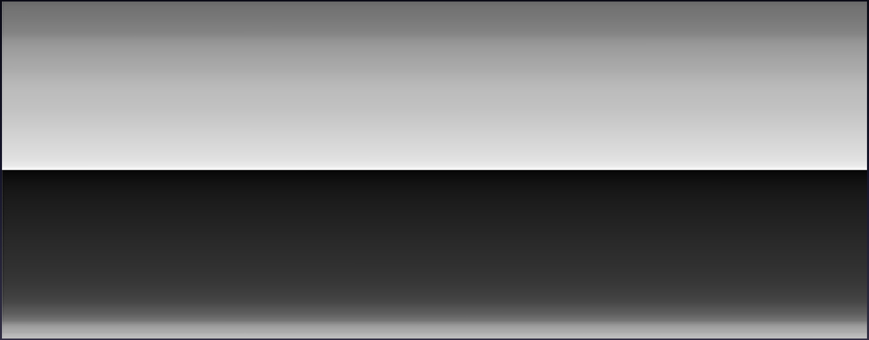
▸ QIndet

Visual artistic representations (Anna Gardner)

Maple vs. Vienna

▸ VisualRep

Visual artistic representations (Anna Gardner)



Mathematica vs. Quantis

VisualRep