How Random is Quantum Randomness?

Cristian S. Calude
University of Auckland

Asian Logic Conference, Wellington, December 2011

What is quantum randomness?

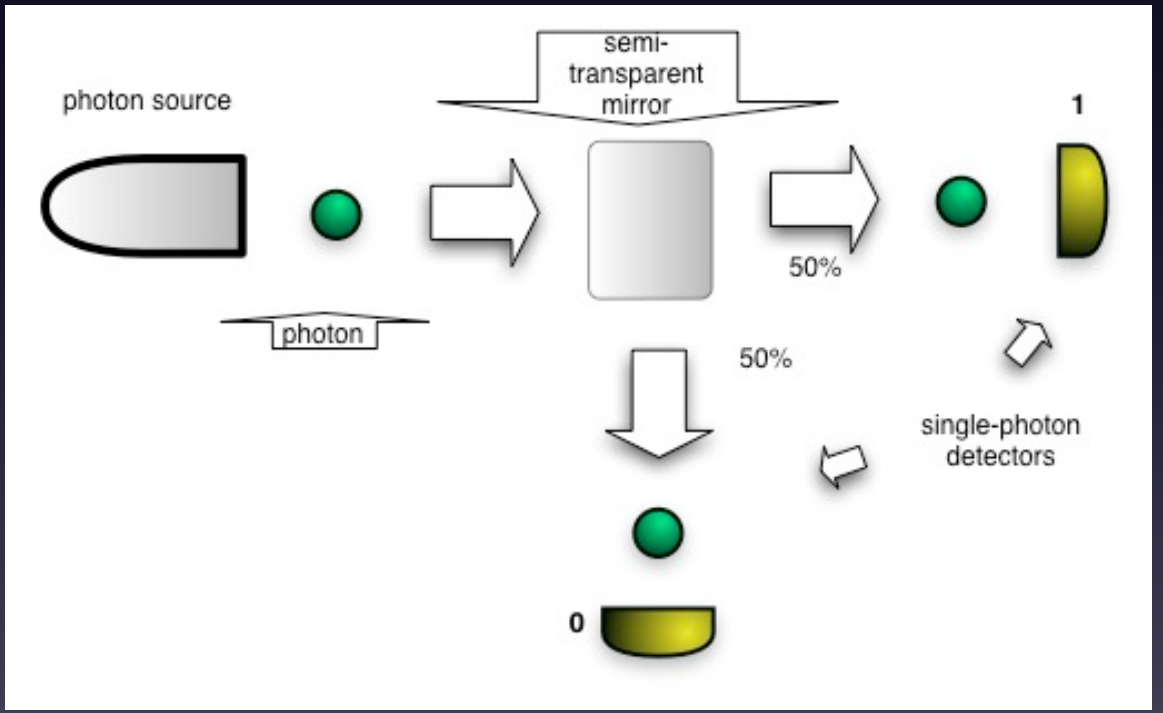
Quantum randomness appears in two different scenarios:

(i) the complete impossibility to predict or explain the occurrence of certain *single* events and measurement outcomes from any kind of operational causal connection, and

(ii) the concatenation of such single quantum random events forms sequences of random bits whith the least correlations, as the occurrence of a particular bit value in a binary expansion does not depend on previous or future bits of that expansion.

Optical quantum randomness

A photon generated by a source beamed to a semi-transparent mirror is reflected or transmitted with 50 per cent chance; measuring, we get a quantum random bit.



Quantum randomness

- has been confirmed by theoretical and experimental research,
- passes all reasonable statistical properties of randomness.

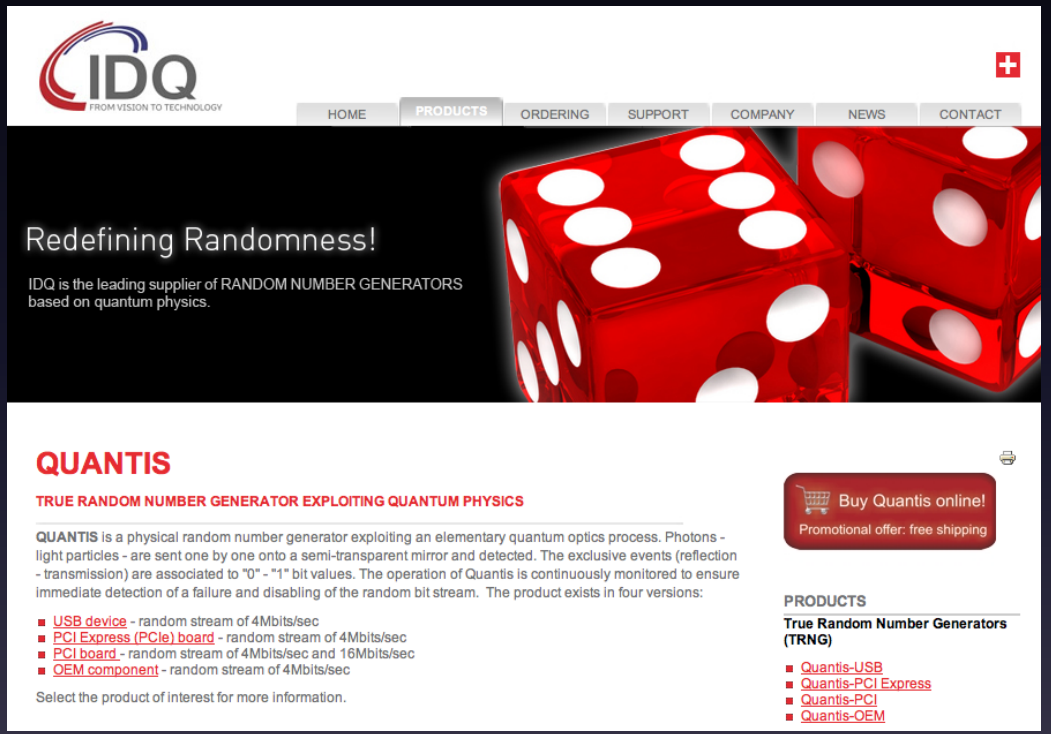
But, where is it coming from?

True randomness?

In spite of mathematics—there is no true randomness—generators of true random bits proliferate.

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

Quantis



Quantis: quantum mechanical random number generator produced and sold by *id Quantique* of the University of Geneva

Quantum indeterminism

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.

Quantum indeterminism

Quantum randomness is not due to ignorance of the system being measured; indeed, since there are in general **no definite values** associated with the measured observable it is surprising there is an outcome at all.

Quantum randomness incomputability

Assume

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

Quantum randomness incomputability

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:

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

Normality test

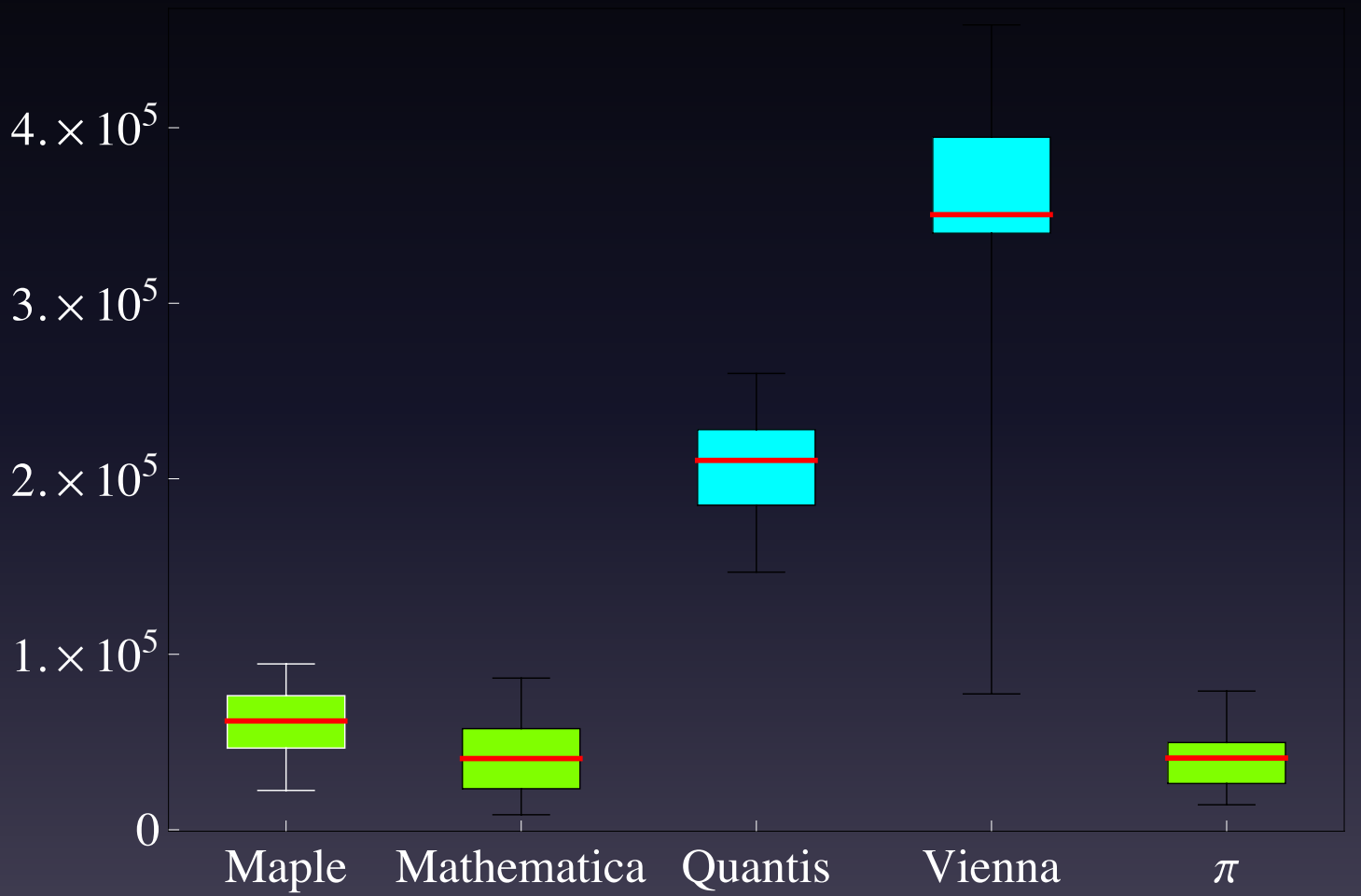
For any fixed integer $m > 1$, $B_m = \{0,1\}^m$, and for every $1 \leq i \leq 2^m$ denote by N_i^m the number of occurrences of the lexicographical ith binary string of length m in the string x over B_m. By $|x|_m$ we denote the length of x

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

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

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

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	$< \mathbf{10^{-4}}$	**0.0002**	0.1678
Mathematica		$< \mathbf{10^{-4}}$	**0.0002**	0.9945
Quantis			**0.0002**	$< \mathbf{10^{-4}}$
Vienna				**0.0002**

Open problems

- Find other principles certifying quantum randomness.
- Is quantum randomness certified by Kochen-Specker theorem Kurtz random? (A real which is contained in every c.e. open set U of measure one is called Kurtz random.)
- Are all forms of quantum randomness equal in quality?

References

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

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.

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