



Libraries and Learning Services

# University of Auckland Research Repository, ResearchSpace

## Version

This is the Author's Original version (preprint) of the following article. This version is defined in the NISO recommended practice RP-8-2008

<http://www.niso.org/publications/rp/>

## Suggested Reference

Calude, C. S., Dinneen, M. J., Dumitrescu, M., & Svozil, K. (2009). *How Random Is Quantum Randomness? An Experimental Approach: Arxiv* (0912.4379v1).

<http://arxiv.org/abs/0912.4379v1>

## Copyright

Items in ResearchSpace are protected by copyright, with all rights reserved, unless otherwise indicated. Previously published items are made available in accordance with the copyright policy of the publisher.

For more information, see [General copyright](#), [Publisher copyright](#).

# **How Random Is Quantum Randomness?**

## **An Experimental Approach**

Cristian S. Calude\* and Michael J. Dinneen†

*Department of Computer Science, University of Auckland,*

*Private Bag 92019, Auckland, New Zealand*

Monica Dumitrescu

*Faculty of Mathematics and Computer Science, University of Bucharest,*

*Str. Academiei 14, 010014 Bucharest, Romania‡*

Karl Svozil

*Institute for Theoretical Physics, University of Technology Vienna,*

*Wiedner Hauptstrasse 8-10/136, 1040 Vienna, Austria§*

(Dated: December 22, 2009)

arXiv:0912.4379v1 [quant-ph] 22 Dec 2009

## Abstract

Our aim is to experimentally study the possibility of distinguishing between quantum sources of randomness—recently proved to be theoretically incomputable—and some well-known computable sources of pseudo-randomness. Incomputability is a necessary, but not sufficient “symptom” of “true randomness.” We base our experimental approach on algorithmic information theory which provides characterizations of algorithmic random sequences in terms of the degrees of incompressibility of their finite prefixes. Algorithmic random sequences are incomputable, but the converse implication is false. We have performed tests of randomness on pseudo-random strings (finite sequences) of length  $2^{32}$  generated with software (Mathematica, Maple), which are cyclic (so, strongly computable), the bits of  $\pi$ , which is computable, but not cyclic, and strings produced by quantum measurements (with the commercial device Quantis and by the Vienna IQOQI group). Our empirical tests indicate quantitative differences, some statistically significant, between computable and incomputable sources of “randomness.”

PACS numbers: 03.67.Lx, 05.40.-a, 03.65.Ta, 03.67.Ac, 03.65.Aa

Keywords: quantum randomness, quantum indeterminism, random processes, quantum algorithms

---

\*cristian@cs.auckland.ac.nz; <http://www.cs.auckland.ac.nz/~cristian>

†mjd@cs.auckland.ac.nz; <http://www.cs.auckland.ac.nz/~mjd>

‡mdumi@fmi.unibuc.ro; [http://fmi.unibuc.ro/ro/dumitrescu\\_monica](http://fmi.unibuc.ro/ro/dumitrescu_monica)

§svozil@tuwien.ac.at; <http://tph.tuwien.ac.at/~svozil>

## I. INTRODUCTION

From the 16th century onwards, following Galilei, Kepler, Leibniz, Newton and others, the rise of determinism culminated around the time of the French and American Revolutions with Laplace’s research on the stability of the solar system without divine intervention [1]. In the late 19th century, first indications of potential limits to the pure deterministic research program emerged, in particular with Poincaré’s contribution [2, 3] to the solution of the three- [4] and general  $n$ -body problem [3, 5, 6], which is often considered as a precursor of chaos theory [7, 8].

Soon, and despite the reluctance and opposition of many of its creators, most notably Planck [9], Einstein [10], Schrödinger and De Brogli, quantum mechanics began to be accepted as an irreducibly probabilistic theory, postulating an indispensable “objective” (in distinction to “epistemic;” cf. below) random behavior of individual particles, while their probabilities follow deterministic laws. With the rise of quantum mechanics (and later on also chaos theory), the *principle of sufficient reason* — stating that every phenomenon has its explanation and cause — had to be partially abandoned. Indeed, indeterminism and randomness in quantum mechanics, as postulated by Born, Heisenberg, Bohr and Pauli [11, p. 115] is commonly believed, accepted and canonized to the extent that [12] “the discovery that individual events are irreducibly random is probably one of the most significant findings of the twentieth century. [[. . .]] for the individual event in quantum physics, not only do we not know the cause, there is no cause.”

However, insufficient causation needs not be perceived merely negatively as a lack of prediction or control. Today it is widely acknowledged that certified randomness can be a valuable resource (e.g., for testing primality [13, 14]), and that under various circumstances a lack of randomness may have negative consequences (e.g., erroneous numerical calculations [15]). The pitfalls of software-generated pseudo-randomness [16] are well-known [15, 17–19]. In John von Neumann’s words [20]: “Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.”

Classical physical processes are subject to difficulties with “subjective” or “epistemic” randomness (a criticism often attributed to Heisenberg [12]) — people consider events to be random when they cannot detect any regularities characterizing the structure of those events, yet the events *could* still be causally described if they would know enough about the evolution of the system — or even bias; the typical example being coin tosses [21]. Several methods to generate random sequences from physical processes have been proposed [22], among them the coding of electric pulses [23],

or semiconductor devices [24–32]. The first book [33] containing a million of random digits using a physical source of randomness was published by The RAND Corporation in 1955 [34].

Currently there are two main sources capable of generating very fast large amounts of “random” bits: software-generated randomness (pseudo-randomness) and quantum randomness. Quantum randomness has been used as an “objective” resource of randomness through various processes, in particular the decay of meta-stable states [35–37] (for a criticism, see [38]) or radioactive decays [39, 40], arrival times [29–32, 41], or the passage through some beam splitter [42–50].

How different are these sources? Recently it has been proved that quantum randomness is incomputable (see more details in Section II D). Incomputability is a necessary, but not sufficient “symptom” of “true randomness.” Can we experimentally distinguish between quantum and computable sources of “randomness?” In what follows, we answer this question in the affirmative using an experimental approach based on algorithmic information theory which provides characterizations of algorithmic random sequences in terms of the degrees of incompressibility of their finite prefixes. Algorithmic random sequences are incomputable, but the converse implication is false.

We have performed tests of randomness on pseudo-random strings (finite sequences) of length  $2^{32}$  generated with software (Mathematica, Maple), which are cyclic (so, strongly computable), the bits of  $\pi$ , which is computable, but not cyclic, and strings produced by quantum measurements (with the commercial device Quantis and by the Vienna IQOQI group).

The paper is organized as follows. In the following section we present quantum randomness; in Section III we present the main tests and results; Section IV includes our conclusions.

## II. QUANTUM RANDOMNESS

In three distinct but intricately interlinked ways, the evolution of quantum mechanics ordained the abandonment of absolute determinism, and has established a clearly defined mixture of determinism and indeterminism, at least in the mainstream perception of the formalism [51–55]:

- (i) random occurrence of individual events [56, 57] or outcomes for quantized systems which are in a superposition of eigenstates of the hermitean operator corresponding to the observable; i.e., randomness from projection measurements on superposition states;
- (ii) complementarity, as proposed by Pauli [58], Heisenberg, Dirac and Bohr;

(iii) value indefiniteness [59] as implied by the theorems of Bell, Kochen & Specker and Greenberger, Horne & Zeilinger [60].

#### **A. Random individual measurement outcomes**

With respect to the perception of certain individual outcomes of measurements, the year 1926 marked the emergence of Born's acausal, indeterministic and probabilistic interpretation of Schrödinger's wave function as a complete and maximal description of a quantum mechanical state. Born states that (cf. [56, p. 866], English translation in Ref. [61, p. 54]) [62],

“From the standpoint of our quantum mechanics, there is no quantity which in any individual case causally fixes the consequence of the collision; but also experimentally we have so far no reason to believe that there are some inner properties of the atom which condition a definite outcome for the collision. Ought we to hope later to discover such properties [[. . .]] and determine them in individual cases? Or ought we to believe that the agreement of theory and experiment — as to the impossibility of prescribing conditions? I myself am inclined to give up determinism in the world of atoms.”

While postulating a probabilistic behavior of individual particles, Born offers a deterministic evolution of the wave function (cf. [57, p. 804], English translation in Ref. [51, p. 302]) [63],

“The motion of particles conforms to the laws of probability, but the probability itself is propagated in accordance with the law of causality. [This means that knowledge of a state in all points in a given time determines the distribution of the state at all later times.]”

At the time of writing this statement Born did not specify the formal notion of “indeterminism” he was relating to. So far, no mathematical characterization of quantum randomness has been proven. In the absence of any indication to the contrary, it is mostly implicitly assumed that quantum randomness is of the strongest possible type; which amounts to postulating that the associated sequences are algorithmically incompressible. This does not exclude the possibility of weaker forms of randomness being generated by quantum measurements.

Random individual outcomes may occur at least in two different ways: (i) either due to a context mismatch between preparation and measurement, (ii) or due to an ignorance of the state preparation resulting in a mixed state. In what follows, we shall discuss these issues in some detail.

We shall consider normalized states. The superscript “ $T$ ” indicates transposition. If not stated otherwise, we shall adopt the notation of Mermin’s book on *Quantum Computer Science* [64]. A quantum mechanical context [65] is a “maximal collection of co-measurable observables” constituting a “classical mini-universe” within the nondistributive structure of quantum propositions. It can be formalized by a single “maximal” self-adjoint operator. Every collection of mutually compatible co-measurable operators (such as projections corresponding to yes–no propositions) are functions of such a maximal operator (e.g., Ref. [66, Sec. II.10, p. 90, English translation p. 173], Ref. [67, § 2], Ref. [68, pp. 227,228], and Ref. [69, § 84]).

### 1. Mismatch between state preparation and measurement

There might be a *context* mismatch between state preparation and measurement; i.e., the system has been prepared in a pure state corresponding to a certain context (maximal observable), and is measured in another, complementary (see below) context (maximal observable). In such a case, the state of the system — in terms of the spectral decomposition of the measurement context — is in a *coherent* superposition of at least some eigenstates of the preparation context. An “irreversible” measurement [70, 71] “reduces” the state to one of the eigenstates of the measurement context. According to the Born rule (e.g., [64, Chapter 1]), the probability of the occurrence of any such measurement outcome labelled by  $i$  is given by the absolute square of the scalar products  $|\langle \psi_i | \varphi \rangle|^2$  between the state  $|\varphi\rangle$  in which the system has been prepared and the corresponding eigenstate  $|\psi_i\rangle$  of the context. Other than this probabilistic law, quantum mechanics renders no further prediction for the occurrence of single measurement outcomes. Note that the amount of indeterminacy (as measured by the lack of bias of measurement outcomes formalizable in terms of average algorithmic information increase per outcome) increases with the “apartness” of the preparation and measurement properties; i.e., with the magnitude of the context mismatch. On the average, conjugate bases [72, p. 86] assure the greatest context mismatch, and hence the greatest degree of randomness gain per experiment.

Quantum realizations of the method have been proposed [42, 43], patented [73] and realized [44, Fig. 1(b)] (see also [45]) for a delayed choice Bell-type experiment [74]. Note that

in the latter experimental realization, in the second *modus operandi* of [74], light of very low intensity — the photon production rate should be much smaller than the corresponding coherence time — is prepared by sending it through a linear polarizer, e.g., in the vertical direction  $\uparrow$ , which guarantees that (ideally) only photons in a definite, pure state corresponding to the polarization direction  $\uparrow$  leave the polarizer. The photons impinge on a beam-splitting polarizer, which should (ideally) be maximally (anti)aligned at exactly  $45^\circ$  ( $\pi/4$  radians) in order to yield a 50:50 ratio of photons polarized in either one of the two orthogonal directions  $\nearrow$  and  $\searrow$  conveyed in the two output ports and detected thereafter, respectively.

The process can be formalized as follows. For a two-state process, a two-dimension Hilbert space suffices. The role of the beam splitter can be described by a very general unitary transformation which can be represented by the product of a  $U(1)$  phase  $e^{-i\beta}$  and of a unimodular unitary matrix  $SU(2)$  [75]

$$\mathbf{T}(\omega, \alpha, \varphi) = \begin{pmatrix} e^{i\alpha} \cos \omega & -e^{-i\varphi} \sin \omega \\ e^{i\varphi} \sin \omega & e^{-i\alpha} \cos \omega \end{pmatrix}, \quad (1)$$

where  $-\pi \leq \beta, \omega \leq \pi$ ,  $-\frac{\pi}{2} \leq \alpha, \varphi \leq \frac{\pi}{2}$ . For our purpose, it suffices to consider a 50:50 beam splitter [76–79] of the Hadamard form  $\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ , which can be obtained from the general form by setting  $\omega = \frac{\pi}{4}$  and  $\alpha = \beta = \gamma = -\frac{\pi}{2}$  in  $e^{-i\beta}$  and in Eq. (1). Note that  $\mathbf{H} \cdot \mathbf{H} = \mathbb{I}_2$  is just the identity matrix in two dimensions.

If  $|\nearrow\rangle \equiv (1, 0)^T$  and  $|\searrow\rangle \equiv (0, 1)^T$  — alternatively, we could have used the notation  $|0\rangle$  for  $|\nearrow\rangle$ , and  $|1\rangle$  for  $|\searrow\rangle$  — represent certain orthogonal (linear polarization) states measured, and the particle has been prepared for in a (linear polarization) state

$$|\uparrow\rangle = \mathbf{H}|\nearrow\rangle = \frac{1}{\sqrt{2}} (|\nearrow\rangle + |\searrow\rangle) \equiv \frac{1}{\sqrt{2}}(1, 1)^T, \quad (2)$$

which is a 50:50 superposition of both of these states, then the probability to find the particle in either one of the detectors corresponding to  $|\nearrow\rangle$  and  $|\searrow\rangle$  is

$$\begin{aligned} P_{\uparrow}(0) &= \text{Tr} [ |\uparrow\rangle\langle\uparrow| \cdot |\nearrow\rangle\langle\searrow| ] \equiv \text{Tr} \left[ \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right] = \frac{1}{2}, \text{ and} \\ P_{\uparrow}(1) &= \text{Tr} [ |\uparrow\rangle\langle\uparrow| \cdot |\searrow\rangle\langle\searrow| ] \equiv \text{Tr} \left[ \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \right] = \frac{1}{2}, \end{aligned} \quad (3)$$

that is, one obtains a 50:50 chance for the occurrence of outcome 0 or 1, respectively.



In general it will be very difficult to establish and maintain an exact (anti)alignment of the polarizers, resulting in a bias towards either state  $|\nearrow\rangle$  or  $|\nwarrow\rangle$ . If and only if this bias is stationary and the events are independent; i.e., uncorrelated, then the bias can be eliminated after the coding stage by von Neumann’s normalization procedure [80]: The biased raw sequence of zeroes and ones is partitioned into fixed subsequences of length two; then the even parity sequences “00” and “11” are discarded, and only the odd parity ones “01” and “10” are kept. In a second step, the remaining sequences could be mapped into the single symbols  $01 \mapsto 0$  and  $10 \mapsto 1$ , thereby extracting a new unbiased sequence at the cost of a loss of original bits [20, p. 768] (see Refs. [81, 82] for an improvement of this method, and Refs. [41, 83, 84] for a discussion of other methods). This method fails if the events are (temporally) correlated and thus not independent. Take, for instance, the sequences  $010101\dots$  or  $101010\dots$ , which in the von Neumann scheme get transformed into  $000\dots$  or  $111\dots$ . Less spectacular failures of the von Neumann normalization can be constructed by considering convex combinations of these cases.

For beam splitters, the independence of outcomes required by the von Neumann normalization translates into the assumption that there are no temporal correlations. In view of the Hanbury Brown Twiss effect (cf., Ref. [85, p.313] and Ref. [86, p.127 ff]), this assumption is highly non-trivial, as effects of photon bunching might disturb the assumption of independence of subsequent “quantum coin tosses.” In particular, it seems that the bit rate might affect the long term statistical independence. Note also that the von Neumann normalization (cf. above) would fail because of the lack of independence [20, p. 768]. Indeed, for “very high” (with respect to the regime of the Hanbury Brown Twiss effect) data rates, independence can no longer be assumed.

## 2. *Ignorance resulting in a mixed state*

A second, maybe faster and technically less demanding possibility to produce quantum random bits does not require any preparation step, but just *assumes* the input state to be principally unknowable and indeterminate. In this case, the system is in a non-pure, mixed state, reflecting our ignorance about the state prepared [87, 2nd part, § 10, p. 827].

If the particle is in a totally mixed state, its density matrix is just proportional to the identity matrix  $\rho_{\mathbb{I}_2} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \equiv \frac{1}{2} \text{diag}[(1,0) + \text{diag}(0,1)] = \frac{1}{2}\mathbb{I}_2$ , and thus the probability to

find the particle in either one of the detectors corresponding to  $|0\rangle$  and  $|1\rangle$  is

$$\begin{aligned} P_{\rho_{\mathbb{I}_2}}(0) &= \text{Tr}[\rho_{\mathbb{I}_2} \cdot |0\rangle\langle 0|] \equiv \text{Tr}\left[\frac{1}{2}\mathbb{I}_2 \cdot \text{diag}(1, 0)\right] = \frac{1}{2}, \text{ and} \\ P_{\rho_{\mathbb{I}_2}}(1) &= \text{Tr}[\rho_{\mathbb{I}_2} \cdot |1\rangle\langle 1|] \equiv \text{Tr}\left[\frac{1}{2}\mathbb{I}_2 \cdot \text{diag}(0, 1)\right] = \frac{1}{2}; \end{aligned} \quad (4)$$

that is, one again obtains a 50:50 chance for the occurrence of outcome 0 or 1, respectively.

Alas, it may be difficult to certify, control and assert “ontologically objective,” as compared to “epistemically subjective,” ignorance. Indeed, the experimenter preparing the system may *subjectively* assume to be ignorant, whereas the system may implicitly be in a pure state with respect to a certain context, of which the experimenter does not possess any knowledge, nor has any control. Also temporal correlations may interfere with randomness.

Note also that any beam splitter is essentially a reversible, one-to-one “translation device” “funneling in” particles in a certain state, thereby transforming the state and “spitting out” the particles in a bijective manner. This is reflected in the unitarity of its quantum mechanical description by the product of  $e^{-i\beta}$  and Eq. (1). Ideally, the original signal can be reconstructed and recovered by the serial composition of the original beam splitter and its “inverse” beam splitter associated with the inverse unitary transformation. In this sense any quantum random number sequence based on beam splitters is as good as the original source of particles, regardless of the successive (quasi-irreversible) measurement by detectors.

For the sake of demonstration, consider a “black box” which, for undisclosed reasons, contains an (unknown) cyclic particle source or, if one prefers, a mischievous demon constantly releasing particles (emanating from the black box) whose states oscillate between  $|0'\rangle = \mathbf{H}|0\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle) \equiv (1/\sqrt{2})(1, 1)^T$  and  $|1'\rangle = \mathbf{H}|1\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle) \equiv (1/\sqrt{2})(1, -1)^T$ , with some frequency  $\nu$ , such that the state as a function of time is either (pure case)

$$|\phi_\nu(t)\rangle = \sin(2\pi\nu t)|0'\rangle + \cos(2\pi\nu t)|1'\rangle, \quad (5)$$

or (mixed case)

$$\rho_\nu(t) = \sin(2\pi\nu t)|0'\rangle\langle 0'| + \cos(2\pi\nu t)|1'\rangle\langle 1'|. \quad (6)$$

If the sampling frequency (or any integer multiple thereof) of this “random” sequence does not coincide with the oscillation frequency  $\nu$ , then it may be very difficult for an experimenter to determine the source’s regular behavior, which — through the beam splitter — translates one-to-one into the sequence generated, since  $\mathbf{H}|0'\rangle = \mathbf{H} \cdot \mathbf{H}|0\rangle = |0\rangle$  and  $\mathbf{H}|1'\rangle = \mathbf{H} \cdot \mathbf{H}|1\rangle = |1\rangle$ .

Thus, it is not totally unjustified to state that claims of “objective” randomness have to be cautiously reviewed when particles emanating from an underspecified source are targeted directly towards some beam splitter, as seems to be the case in one of the two setups in Ref. [44, Fig. 1(a)] and for other devices[88]. The quality of the quantum random sequences produced thus seems to depend on the quality of the light source [45] in combination with the beam splitter. While “*for all practical purposes*” it may be justified to use a particular (or maybe even any type of) particle source in combination with a particular beam splitter, this falls short of a certified procedure to obtain truly random bits in accordance with Bohm’s principle of indeterminacy.

## B. Complementary contexts

Complementarity is a quantum resource for randomness which may be supporting the random occurrence of individual events dealing with a mismatch between state preparation and measurement, as has already been discussed in the Section II A 1. It is, however, no sufficient criterion for indeterminism, as can be seen from finite automata [89] or generalized urn models [90], which are nondistributive but still allow a classical representation [91, 92]. Whether or not complementarity is a necessary criterion for quantum indeterminism seems to be debatable. For the lack of necessity, it may suffice to refer to some recording of individual outcomes of “irreversible” measurements associated with a “state reduction,” or to some decay of a meta-stable state. Yet, in the first “state reduction” case, the existence of principally unpredictable outcomes seems to be linked to complementarity; at least from an operational point of view. And also decays of excited states, due to the quantum Zeno effect [93], depend on the mode of their measurement, which may be linked to time and energy. We shall not discuss these issues related to necessity further.

Early discussions of complimentary-type features of quantum mechanics [94, 95] concentrate on a finite form of paradoxical self-reference among complementary observables resembling recursion theoretic diagonalization. In the words of Dirac [96, §1],

“It is usually assumed that, by being careful, we may cut down the disturbance accompanying our observation to any desired extent. The concepts of big and small are then purely relative and refer to the gentleness of our means of observation as well as to the object being described. In order to give an absolute meaning to size, such as is required for any theory of the ultimate structure of matter, we have to assume that there is a limit to the fineness of our powers of observation and the smallness of

the accompanying disturbance—a limit which is inherent in the nature of things and can never be surpassed by improved technique or increased skill on the part of the observer. If the object under observation is such that the unavoidable limiting disturbance is negligible, then the object is big in the absolute sense and we may apply classical mechanics to it. If, on the other hand, the limiting disturbance is not negligible, then the object is small in the absolute sense and we require a new theory for dealing with it.

A consequence of the preceding discussion is that we must revise our ideas of causality. Causality applies only to a system which is left undisturbed. If a system is small, we cannot observe it without producing a serious disturbance and hence we cannot expect to find any causal connexion between the results of our observations. Causality will still be assumed to apply to undisturbed systems and the equations which will be set up to describe an undisturbed system will be differential equations expressing a causal connexion between conditions at one time and conditions at a later time. These equations will be in close correspondence with the equations of classical mechanics, but they will be connected only indirectly with the results of observations. There is an unavoidable indeterminacy in the calculation of observational results, the theory enabling us to calculate in general only the probability of our obtaining a particular result when we make an observation.”

In 1933, Pauli gave the first explicit definition of complementarity stating that (cf. [58, p. 7], partial English translation in Ref. [51, p. 369]) [97],

“In the case of an indeterminacy of a property of a system at a certain configuration (at a certain state of a system), any attempt to measure the respective property (at least partially) annihilates the influence of the previous knowledge of system on the (possibly statistical) propositions about possible later measurement results. [[...]] The impact on the system by the measurement apparatus for momentum (position) is such that within the limits of the uncertainty relations the value of the knowledge of the previous position (momentum) for the prediction of later measurements of position and momentum is lost. If, for this reason, the applicability of *one* classical concept stands in the relation of exclusion to that of *another*, we call both of these concepts (e.g., the position and momentum coordinates of a particle) with Bohr *complemen-*

*tary*. [...] One will see that this “complementarity” has no analogy in the classical statistical theory of gases, which also operates with statistical laws. This theory does not contain the assertion — which is only valid through the finiteness of the quantum of action — that the measurement of a system may necessarily result in a loss of knowledge acquired through previous measurements; i.e., the previous measurements can no longer be used.”

Complementarity may thus be interpreted as a subtle kind of departure from classical omniscience: whereas it may in principle be possible to measure any single, individual context, or any (classically operational) observable within (or encompassing) a context, the direct measurement (not involving counterfactuals in Einstein-Podolsky-Rosen type configurations [98, 99]) of two or more contexts, or of one context and some observable “outside” of it is impossible.

Until the theorems by Bell, Kochen & Specker and Greenberger, Horne & Zeilinger, quantum indeterminism was thus either (i) “believed” and corroborated by the “effective inability to disprove the contrary” (i.e., determinism), or (ii) argued by “intrinsic self-reference” and the impossibility of the measurement process to act “softer than” the quantum of action  $h$  on the object. In the latter case, one could still believe that, contrary to (i), there exist *elements of physical reality*, which, in the sense of Einstein, Podolsky and Rosen [98] could even be measured and counterfactually [99] inferred simultaneously [100].

### C. Value indefiniteness

In deriving the quantum probabilities — which have originally been postulated by Born’s rule as an axiom of quantum mechanics — from a buildup of classical probabilities within contexts in Hilbert spaces of dimension greater than two, Gleason’s theorem [101–104] has motivated many authors to derive nonlocal [59, 60, 74, 105–107] as well as local [67, 108–117] constraints on the existence of *global* truth functions (two-valued measures) on the *entire domain* of quantum observables. Bell’s theorem already statistically indicated the impossibility of co-existence of certain observables “exceeding” a single context, e.g., by considering the statistics of listing of possible measurement outcomes and comparing them to the quantum expectations [59]; and the Kochen-Specker theorem presented a finite proof (by contradiction) of the impossibility of their co-existence.

When it comes to interpreting and understanding these results, one difficulty is a fact already en-

countered in the study of complementarity: whereas the *totality* of contexts is not co-measurable, any *individual* context is measurable. In this sense, the Kochen-Specker and related [60, 107] theorems can be viewed to strengthen complementarity: not only is it *operationally* impossible to directly [100] measure more than a single context (despite counterfactual measurements of two contexts in Einstein-Podolsky-Rosen type configurations [98, 99]) — it is provable impossible to consistently assume any co-existence of all quantum observables which could in principle be measured [59]. We shall refer to this as *value indefiniteness*.

Of course, there are ways to “cope” with these findings quasi-classically (quasi-realistically) the most popular being the “contextuality” assumption, which was first put forward by Bell in an attempt to save a kind of realism [106, 118–120]. It maintains the physical existence of all conceivable potential observables but assumes that the [119] “... result of an observation may reasonably depend not only on the state of the system . . . but also on the complete disposition of the apparatus,” which could mean that the outcome of a measurement may depend on its context [121].

Note that, due to the Born rule — derivable by Gleason’s theorem [101, 102, 104] for three- and higher-dimensional Hilbert space — the quantum mechanical expectation value  $\langle E \rangle_\rho = \text{Tr}(\rho E)$  of an observable corresponding to a hermitean operator  $E$  and a physical state  $\rho$  does not depend on the context; in particular, the expectation value  $\langle E \rangle_\rho$  of a proposition corresponding to a projector  $E$  is independent of the particular choice of basis among the continuity of orthogonal bases which it may belong to [122]. Thus, contextuality is restricted to *single, individual outcomes* of potential measurements. Stated differently, quantum mechanics does not determine a specific measurement outcome of an observable, but determines the expectation value of that observable. In this respect, the quantum contextuality assumption is somewhat similar to Born’s concept of deterministic evolution of the quantum state as compared to the indeterministic occurrence of single events; or the *outcome dependence versus parameter independence* for remote nonlocal [123] correlated quantum events [124].

The Kochen-Specker theorem is a rather strong indication of value indefiniteness and thus of quantum indeterminism [125] and randomness beyond Born’s conjecture of the random occurrence of individual events, and even beyond complementarity; at least for multi-context configurations where Kochen & Specker constructions are viable.

Since a nontrivial interconnectedness of different bases is possible only for Hilbert spaces of dimension three onwards, the Gleason and the Kochen-Specker theorems apply only to Hilbert spaces of dimensions *higher than two* (see the related argument in Ref. [126, p. 193]); hence value

indefiniteness can be proven only for systems of *three or more mutually exclusive outcomes*. For two-dimensional systems, one has still to rely purely on Born’s indeterminacy postulate, solely backed by complementarity and the quantum uncertainty relations. We have to conclude that, as presently many quantum random number generators using beam splitters (also the ones utilizing complementarity) operate with two exclusive outcomes, they are not backed by value indefiniteness in the sense of Bell, Kochen & Specker and Greenberger, Horne & Zeilinger.

One may still argue that, although the Born rule for quantum probabilities and expectations cannot be proven from the (more elementary) assumptions of Gleason’s theorem [126, § 7.2] for two-dimensional Hilbert spaces by presently known mathematical methods, this does not exclude the possibility that some other methods exist which would prove similar results related to value indefiniteness even for physical configurations with two mutually exclusive outcomes. For the sake of excluding this latter possibility, one should, for instance, find a counterexample (on the structure of quantum observables in two-dimensional Hilbert space) which (i) either is not in accordance with the Born rule but still in accordance with the additivity property upon which Gleason’s theorem is based; (ii) or is in accordance with the Born rule but allows two-valued states which may or may not be sufficient for a homeomorphic embedding into a Boolean algebra. A typical counterexample of the first type would be one in which an electron spin observable, for noncollinear directions, would always point “up” and “down” according to some algorithmic rule [127, pp. 70-72]). Formally, this is due to the fact that, for two-dimensional configurations, there exists a full, separating set of two-valued states. A counterexample of the second type appears to allow merely states which are singular only in a *single* pair of observables (indeed, this is true for arbitrary Hilbert space dimensions), and thus are insufficient for the particular purpose.

#### **D. Incomputability of quantum randomness and empirical testing**

In [125] it is proved that quantum randomness is not Turing computable. More precisely, suppose that a quantum experiment produces an infinite sequence of quantum random bits. Would such a sequence be computable by a Turing machine? If we accept value indefiniteness as expressed by the theorems of Bell, Kochen & Specker and Greenberger, Horne & Zeilinger, then the answer given in Ref. [125] is negative; even more, *no Turing machine can enumerate an infinity of correct bits of such a sequence*. For example, an infinite sequence of quantum random bits may start with a billion of 0’s, but cannot consist entirely of only 0’s. The infinite sequence of bits

0100011011000001... (Champernowne's constant) or the binary expansion of  $\pi$  cannot be exactly reproduced by any quantum experiment.

But is quantum randomness a “true” and “objective” form of randomness? First, and foremost, there is no such thing as “true” randomness as measure-theoretical arguments show [128]. Secondly, *it is an open question whether quantum randomness satisfies the requirements of algorithmic randomness* [128].

Our aim is to experimentally study the possibility of distinguishing between quantum sources of randomness (proved to be theoretically incomputable) and some well-known computable sources of pseudo-randomness. The legitimacy of the experimental approach comes from algorithmic information theory which provides characterizations of algorithmic random sequences in terms of the degrees of incompressibility of their finite prefixes. More precisely, a sequence is algorithmic random iff all its finite prefixes cannot be compressed by a universal prefix-free Turing machine by more than a fixed constant (which depends on the fixed machine and sequence and not on prefixes) [128]. The degree of incompressibility of a string is measured with the prefix-complexity  $H_U$  (which depends on the universal prefix-free Turing machine  $U$ ). The best empirical test of randomness would be to calculate the prefix-complexity of all prefixes of a given (long) string. This is impossible because the prefix-complexity is incomputable. However, there are computable, but weaker properties than incompressibility which can be tested on prefixes, for example, Borel normality (explained below). Of course, any such property is necessary, but not sufficient; hence the (degree of) *absence of the property is significant*.

We have performed tests of randomness on pseudo-random strings (finite sequences) of length  $2^{32}$  generated with software (Mathematica, Maple), which are not only computable, but also cyclic, the bits of  $\pi$ , which is computable, but not cyclic, and strings produced by quantum measurements with the commercial device Quantis, as well as by the Vienna IQOQI group.

The signals of the Vienna Institute for Quantum Optics and Quantum Information (IQOQI) group were generated with photons from a weak blue LED light source which impinged on a beam splitter without any polarization sensitivity with two output ports associated with the codes “0” and “1,” respectively [44]. There was no pre- or post-processing of the raw data stream, however the output was constantly monitored (the exact method is subject to a patent pending). In very general terms, the setup needs to be running for at least one day to reach a stable operation. There is a regulation mechanism which keeps track of the bias between “0” and “1,” and tunes the random generator for perfect symmetry. Each data file was created in one continuous run of the



device lasting over hours.

Our empirical tests indicate quantitative differences between computable and incomputable sources by examining (long, but) finite prefixes of infinite sequences. Such differences are guaranteed to exist by the result in Ref [125], but, because computability is an asymptotic property, there is no guarantee that finite tests can “pick” them in the prefixes we have analyzed. We performed more tests than those described below, but discarded those for which the results were inconclusive (cf. Ref. [129]). In what follows we will describe a battery of “non-standard” randomness tests based on coding theory and algorithmic information theory results [128] which distinguish between the computable and incomputable sources that we sampled.

### III. RANDOMNESS TESTS

In order to avoid some ideological or metaphysical bias, all sequences have been treated on an equal footing by looking with “evenly-suspended attention” at their phenomenological encoded phenotypes. No hidden “meaning” or “message” should be ascribed to them. This is conceptually related to the following scenario.

Consider a couple of labeled “black boxes,” each being the source of binary sequences, emanated at a constant rate. In our case, we have two “Born boxes” operating under Born’s assumption of quantum randomness (actually, Quantis is just that), a “Pi box” humming out binary digits of  $\pi$ , as well as some “Sinners” (in von Neumann’s judgment [20]) containing algorithms pretending to output random digits.

Suppose that these boxes cannot be “screwed open,” and no clues about the origin of the symbolic sources are otherwise obtainable from the outside in any perceivable way. Suppose further that somebody (either a devil, or a malign colleague, or a cleaning agent) has erased the labels completely. Would we be able to tell which box is which by analyzing their bit renditions alone? In what follows, we shall present some tentative answers to this question based on data produced with these boxes.

#### A. Data

Our data consist of 50 binary sample “random” strings of length  $2^{32}$ : 10 pseudo-random strings produced by Mathematica 6 [130], 10 pseudo-random strings produced by Maple 11 [131], 10

quantum random strings generated with Quantis [132], 10 quantum random strings generated by the Vienna IQOQI group [133], and 10 strings of  $2^{32}$  bits from the binary expansion of  $\pi$  obtained from [134].

The process used to generate ten strings from  $\pi$  is the following. The input was given to us in hexadecimal format, with two decimal digits per byte; or one decimal digit per nibble. Two random decimal digits were selected to be omitted throughout the string [135] The remaining decimal digits are assigned a 3-bit binary number 0 to 7, which are output as 3 bits each. Processing continues until  $2^{32}$  bits are output. The input source that we downloaded had 4,200,000,000 decimal digits so potentially up to  $1.008 \times 10^{10}$  bits can be extracted (which is about  $2.347 \times 2^{32}$ ); thus almost all of these digits are needed to generate our 10 strings. The justification that these “projected” binary strings share the same randomness properties of  $\pi$  is given by the following result [128]: if in a random sequence over an alphabet  $\{a_1, \dots, a_k\}$ ,  $k > 2$ , we remove all occurrences of a fixed symbol  $a_i$ , then the new sequence is also random (over an alphabet with  $k - 1$  symbols).

## B. Descriptive statistics

Our experiments have been uniformly performed on all these fifty sample strings. The tests presented below can be grouped into the following classes:

- (i) Borel normality test;
- (ii) test based on Shannon’s information theory;
- (iii) two tests based on algorithmic information theory; and
- (iv) test based on random walks.

We present our test results using box-and-whisker plots which are compact graphical representations of groups of numerical data through five characteristic summaries: test minimum value, first quantile (representing one fourth of the test data), median or second quantile (representing half of the test data), third quantile (representing three fourths of the test data), and test maximum value. Mean and standard deviation of the data representing the results of the tests are calculated. For the reader who prefers “numbers” instead of “pictures,” tables containing all these seven elements of descriptive statistics are included for all five sources.

Tables containing the experimental data and the programs used to generate the data can be downloaded from our extended paper [136].

### 1. Borel normality test

Borel normality was the first mathematical definition of randomness [137]. A sequence is (Borel) normal if every binary string appears in the sequence with the right probability (which is  $2^{-n}$  for a string of length  $n$ ). A sequence is normal if and only if it is incompressible by any information lossless finite-state compressor [138], so normal sequences are those sequences that appear random to any finite-state machine.

Every algorithmic random infinite sequence is Borel normal [139]. The converse implication is not true: there exist computable normal sequences (e.g. Champernowne's constant).

Normality is invariant under finite variations: adding, removing, or changing a finite number of bits in any normal sequence leaves it normal. Further, if a sequence satisfies the normality condition for strings of length  $n + 1$ , then it also satisfies normality for strings of length  $n$ , but the converse is not true.

Normality was transposed to strings in Ref. [139]. In this process one has to replace limits with inequalities. As a consequence, the above two properties, which are valid for sequences, are no longer true for strings.

For any fixed integer  $m > 1$ , consider the alphabet  $B_m = \{0, 1\}^m$  consisting of all binary strings of length  $m$ , and for every  $1 \leq i \leq 2^m$  denote by  $N_i^m$  the number of occurrences of the lexicographical  $i$ th binary string of length  $m$  in the string  $x$  (considered over the alphabet  $B_m$ ). By  $|x|_m$  we denote the length of  $x$ . A string  $x$  is Borel 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  $1 \leq j \leq 2^m$ . In Ref. [139] it is shown that almost all algorithmic random strings are Borel normal.

In the first test we count the maximum, minimum and difference of non-overlapping occurrences of  $m$ -bit ( $m = 1, \dots, 5$ ) strings in each sample string. Then we tested the Borel normality property for each sample string and found that almost all strings pass the test, with some notable exceptions. We found that several of the Vienna sequences failed the expected count range for  $m = 2$  and a few of the Vienna sequences were outside the expected range for  $m = 3$  and  $m = 4$

TABLE I. Statistics for the results for tests of the Borel normality property.

Descriptive statistics	min	Q1	median	Q3	max	mean	sd
Maple	22430	47170	61990	76130	94510	60210	21933.52
Mathematica	8572	25500	40590	55650	86430	41870	23229.77
Quantis	146800	185100	210500	226600	260000	207200	33515.65
Vienna	77410	340200	350500	392500	260000	337100	103354.3
$\pi$	14260	28860	40880	47860	79030	40220	17906.21

(some less than the expected minimum count and some more than the expected maximum count). The only other bit sequence that was outside the expected range count was one of the Mathematica sequences that had a too big of a count for  $k = 1$ . Figure 1 depicts a box-and-whisker plot of the results. This is followed by statistical (numerical) details in Table I.

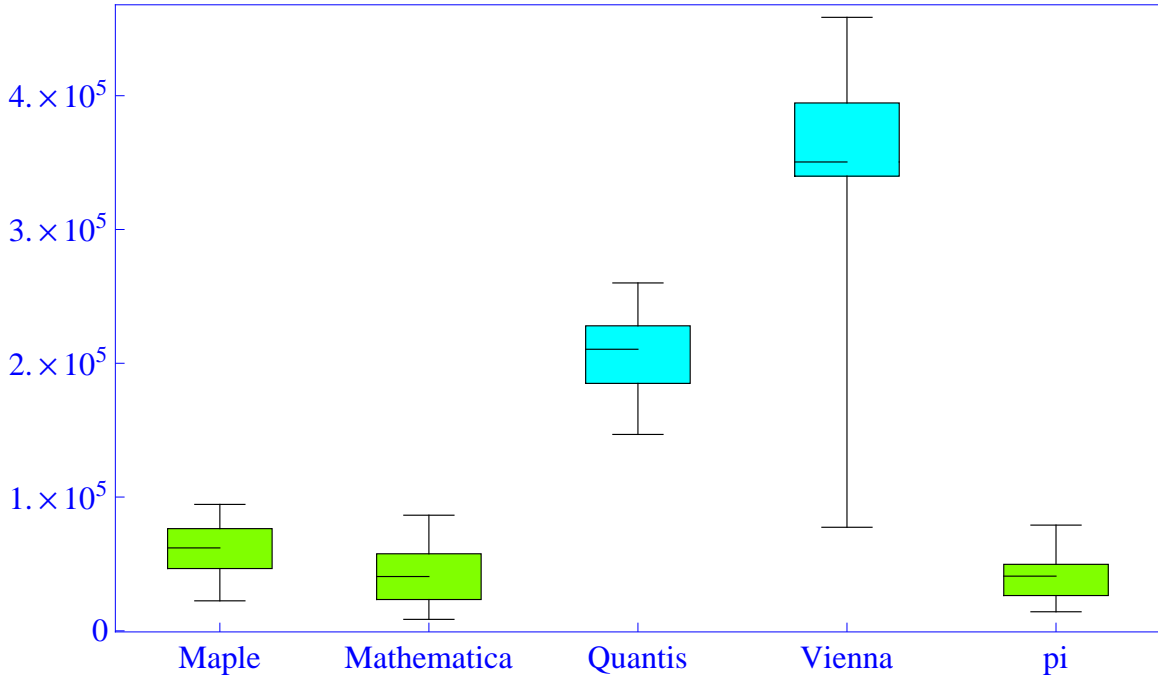


FIG. 1. (Color online) Box-and-whisker plot for the results for tests of the Borel normality property.

TABLE II. Statistics for average results in “sliding window” estimations of the Shannon entropy.

Descriptive statistics	min	Q1	median	Q3	max	mean	sd
Maple	0.9772	0.9781	0.9784	0.9787	0.9788	0.9783	0.0005231617
Mathematica	0.9776	0.9781	0.9783	0.9785	0.9800	0.9783	0.0006654936
Quantis	0.9779	0.9783	0.9783	0.9786	0.9795	0.9784	0.0004522699
Vienna	0.9772	0.9777	0.9784	0.9790	0.9792	0.9783	0.0006955834
$\pi$	0.9779	0.9784	0.9788	0.9790	0.9799	0.9788	0.0006062724

## 2. Test based on Shannon’s information theory

The second test computes “sliding window” estimations of the Shannon entropy  $L_n^1, \dots, L_n^t$  according to the method described in [140]: a smaller entropy is a symptom of less randomness. The results are presented in Figure 2 and Table II.

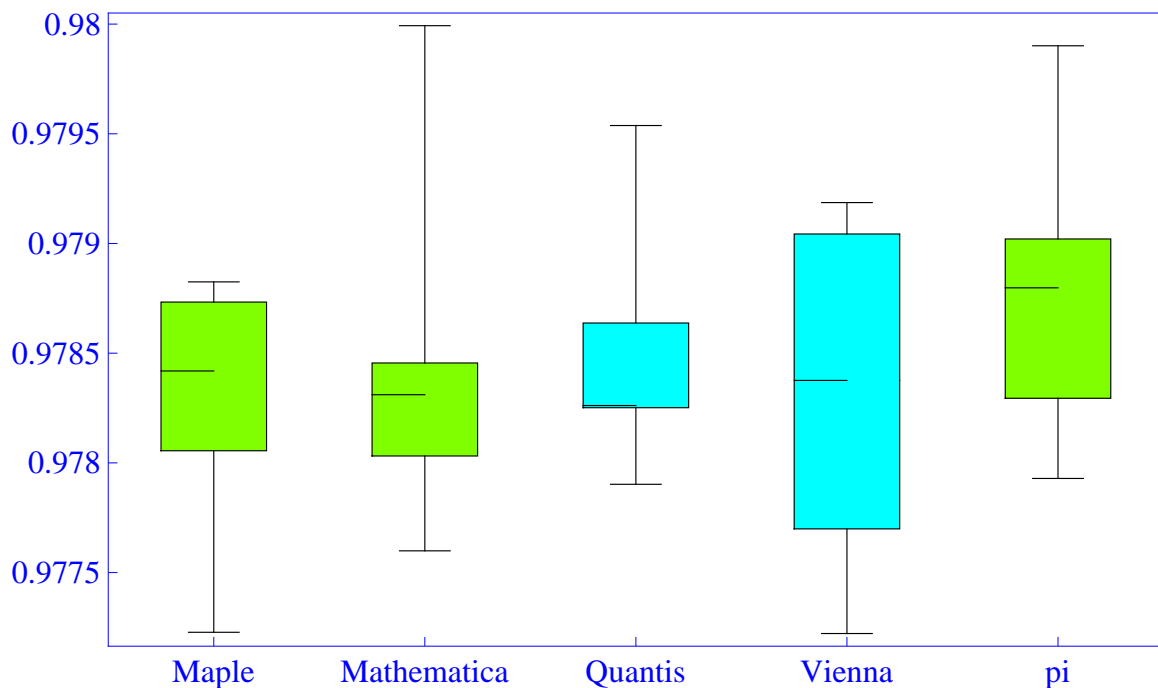


FIG. 2. (Color online) Box-and-whisker plot for average results in “sliding window” estimations of the Shannon entropy.

### 3. Tests based on algorithmic information theory

The third test uses the “book stack” (also known as “move to front”) randomness test as proposed in Ref. [141, 142]. More compression is a symptom of less randomness. The results, presented in Figure 3 and Table III, are derived from the original count, the count after the application of the transformation, and the difference. The key metric for this test is the count of ones after the transformation. The book stack encoder does not compress data but instead rewrites each byte with its index (from the top/front) with respect to its input characters being stacked/moved-to-front. Thus, if a lot of repetitions occur (i.e., a symptom of non-randomness), then the output contains more zeros than ones due to the sequence of indices generally being smaller numerically.

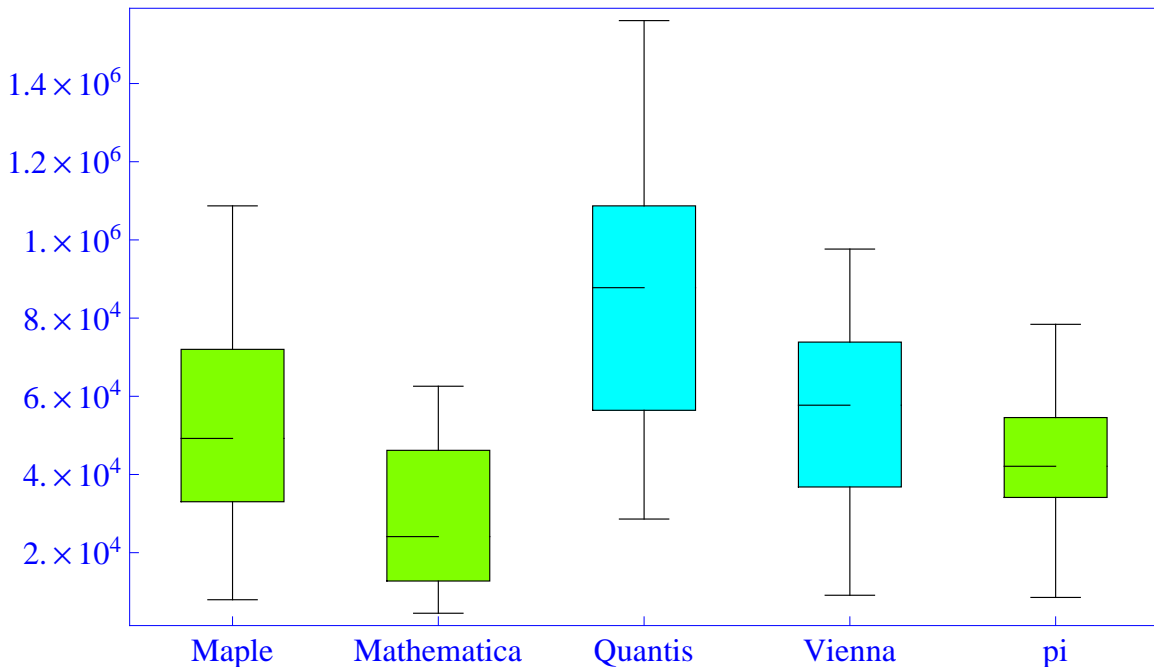


FIG. 3. (Color online) Box-and-whisker plot for the results of the “book stack” randomness test.

The fourth test is based solely on the behavior of algorithmic random strings (as selectors for Solovay-Strassen probabilistic primality test) and not on specific properties of randomness.

To test whether a positive integer  $n$  is prime, we take  $k$  natural numbers uniformly distributed between 1 and  $n - 1$ , inclusive, and, for each one  $i$ , check whether the predicate  $W(i, n)$  holds. If this is the case we say that “ $i$  is a witness of  $n$ ’s compositeness”. If  $W(i, n)$  holds for at least one  $i$  then  $n$  is composite; otherwise, the test is inconclusive, but in this case if one declares  $n$  to be prime then the probability to be wrong is smaller than  $2^{-k}$ .

TABLE III. Statistics for the results of the “book stack” randomness test.

Descriptive statistics	min	Q1	median	Q3	max	mean	sd
Maple	7964	34490	49220	69630	108700	53410	33068.58
Mathematica	4508	13020	24110	43450	62570	27940	19406.03
Quantis	28600	60480	87780	106700	156100	89990	41545.76
Vienna	9110	38420	57720	73220	97660	53860	27938.92
$\pi$	8551	35480	42100	52870	78410	41280	20758.46

This is due to the fact that at least half  $i$ 's from 1 to  $n - 1$  satisfy  $W(i, n)$  if  $n$  is indeed composite, and *none* of them satisfy  $W(i, n)$  if  $n$  is prime [143]. Selecting  $k$  natural numbers between 1 and  $n - 1$  is the same as choosing a binary string  $s$  of length  $n - 1$  with  $k$  1's such that the  $i$ th bit is 1 iff  $i$  is selected. Ref. [13] contains a proof that, if  $s$  is a long enough algorithmically random binary string, then  $n$  is prime iff  $Z(s, n)$  is true, where  $Z$  is a predicate constructed directly from conjunctions of negations of  $W$  [144].

A Carmichael number is a composite positive integer  $k$  satisfying the congruence  $b^{k-1} \equiv 1 \pmod{k}$  for all integers  $b$  relative prime to  $k$ . Carmichael numbers are composite, but are difficult to factorize and thus are “very similar” to primes; they are sometimes called pseudo-primes. Carmichael numbers can fool Fermat’s primality test, but less the Solovay-Strassen test. With increasing values, Carmichael numbers become “rare” [145].

The fourth test uses Solovay-Strassen probabilistic primality test for Carmichael numbers (composite) with prefixes of the sample strings as the binary string  $s$ . We used the Solovay-Strassen test for all Carmichael numbers less than  $10^{16}$ —computed in Ref. [146, 147]—with numbers selected according to increasing prefixes of each sample string till the algorithm returns a non-primality verdict. The metric is given by the length of the sample used to reach the correct verdict of non-primality for all of the 246683 Carmichael numbers less than  $10^{16}$ . [We started with  $k = 1$  tests (per each Carmichael number) and increase  $k$  until the metric goal is met; as  $k$  increases we always use new bits (never recycle) from the sample source strings.] The results are presented in Figure 4 and Table IV.

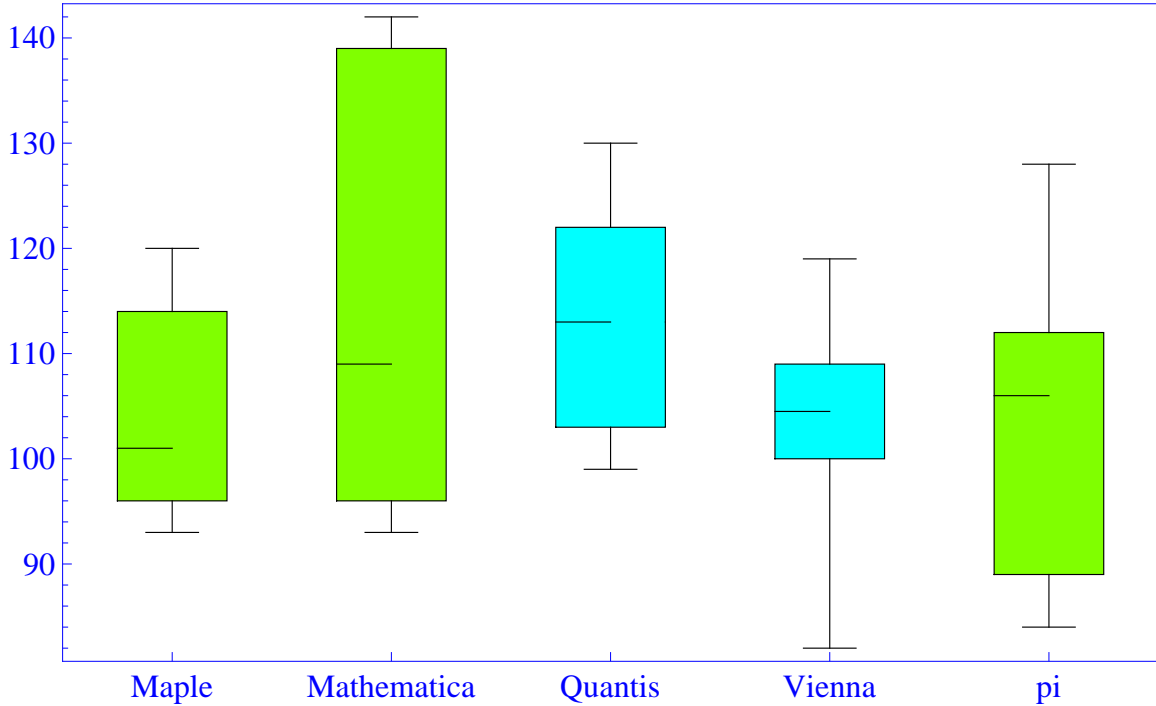


FIG. 4. (Color online) Box-and-whisker plot for the results based on the Solovay-Strassen probabilistic primality test.

TABLE IV. Statistics for the results based on the Solovay-Strassen probabilistic primality test.

Descriptive statistics	min	Q1	median	Q3	max	mean	sd
Maple	93.0	96.0	101.0	113.5	120.0	104.9	10.57723
Mathematica	93.0	97.0	109.0	132.3	142.0	113.5	19.60867
Quantis	99.0	103.3	113.0	121.3	130.0	112.6	10.66875
Vienna	82.0	100.3	104.5	109.0	119.0	103.5	11.03781
$\pi$	84.0	91.75	106.0	110.8	128.0	104.7	10.66875

#### 4. Test based on random walks

A symptom of non-randomness of a string is detected when the plot generated by viewing a sample sequence as a 1D random walk meanders less away from the starting point (both ways); hence the max-min range is the metric.

The fifth test is based on viewing a random sequence as a 1D random walk. Here the bits



TABLE V. Statistics for the results of the random walk tests.

Descriptive statistics	min	Q1	median	Q3	max	mean	sd
Maple	67640	88730	126400	162500	180500	125300	42995.59
Mathematica	73500	84760	98110	103400	120300	96450	14685.34
Quantis	138200	161600	209000	250200	294200	211300	55960.23
Vienna	92070	130200	155600	167600	226900	152900	36717.55
$\pi$	58570	70420	82800	91920	107500	82120	14833.75

(indices along the  $x$ -axis) are interpreted as follows: 1=move up, 0=move down ( $y$ -axis). This test measures how far away from the starting point (in either positive or negative) from the starting  $y$ -value of 0 that one can reach using successive bits of the sample sequence. Figure 5 and Table V summarize the results.

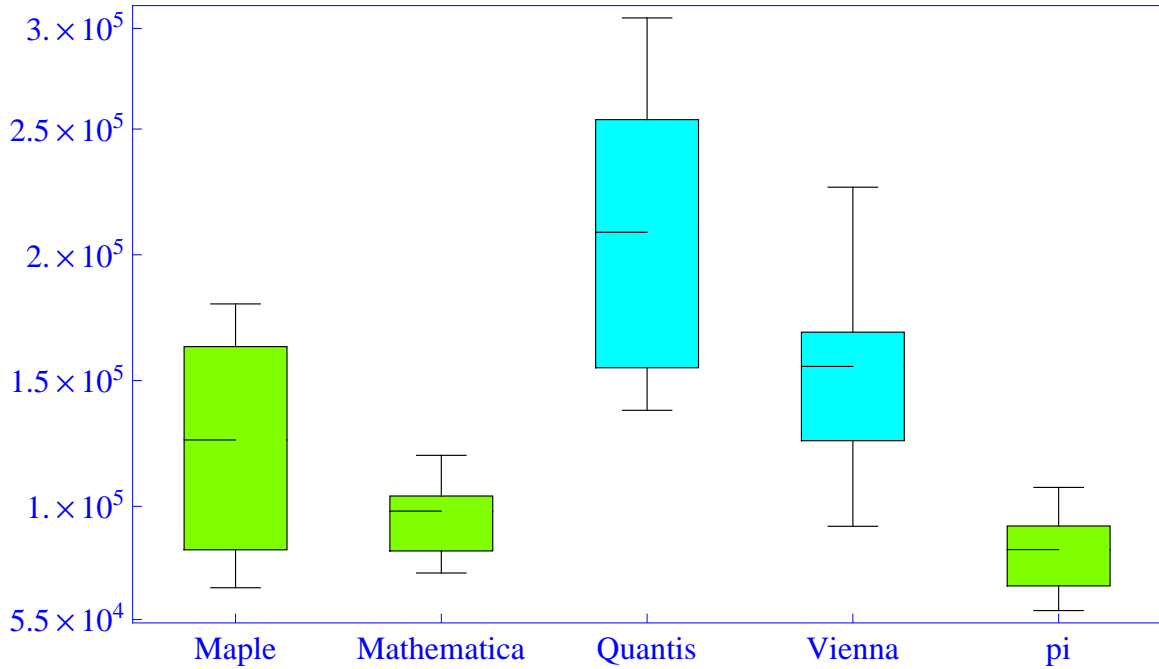


FIG. 5. (Color online) Box-and-whisker plot for the results of the random walk tests.

### C. Statistical analysis of randomness tests results

In what follows statistical tests are used to compare the probability distributions of results of randomness tests applied to the strings generated by the five sources. The Kolmogorov-Smirnov test for two samples [148] tries to determine if two datasets differ significantly. This test has the advantage of making no assumption about the distribution of data; i.e., it is non-parametric and distribution free. The Kolmogorov-Smirnov test returns a  $p$ -value, and the decision “the difference between the two datasets is statistically significant” is accepted if the  $p$ -value is *less than* 0.05; or, stated pointedly, if the probability of taking a wrong decision is less than 0.05. Exact  $p$ -values are only available for the two-sided two-sample tests with no ties.

In some cases we have tried to double-check the decision “no significant differences between the datasets” at the price of a supplementary, plausible distribution assumption. Therefore, we have performed the Shapiro-Wilk test for normality [149] and, if normality is not rejected, we have assumed that the datasets have normal (Gaussian) distributions. In order to be able to compare the expected values (means) of the two samples, the Welch  $t$ -test [150], which is a version of Student’s test, has been applied.

The Shapiro-Wilk test examines the null hypothesis that a sample  $z_1, \dots, z_n$  comes from a normally distributed population. This test is appropriate for small samples, since it is not an asymptotic test. As for each source ten independent strings have been studied, we have applied the Shapiro-Wilk test for a sample size  $n = 10$ .

The Welch’s  $t$ -test [150] is an adaptation of Student’s  $t$ -test used with two samples having possibly unequal variances. It is used to test the null hypothesis that the two population means are equal (using a two-tailed test).

The calculations have been performed with the software “R” [151]. In order to emphasize the relevance of  $p$ -values less than 0.05 associated with Kolmogorov-Smirnov, Shapiro-Wilk and Welch’s  $t$ -tests, they are printed in boldface and discussed in the text.

#### 1. Borel test of normality

The results of the Kolmogorov-Smirnov test are presented in Table VI.

Statistically significant differences are identified for (i) Quantis *versus* Maple, Maple, Mathematica and  $\pi$ ; (ii) Vienna *versus* Maple, Mathematica and  $\pi$ ; and (iii) Quantis *versus* Vienna.

TABLE VI. Kolmogorov-Smirnov test for the Borel normality tests.

Kolmogorov-Smirnov test $p$ -values	Mathematica	Quantis	Vienna	$\pi$
Maple	0.4175	$< 10^{-4}$	<b>0.0002</b>	0.1678
Mathematica		$< 10^{-4}$	<b>0.0002</b>	0.9945
Quantis			<b>0.0002</b>	$< 10^{-4}$
Vienna				<b>0.0002</b>

Note that

- (i) Pseudorandom strings pass the Borel normality test for comparable numbers of counts, relatively small: if the angle brackets  $\langle x \rangle$  stand for the statistical mean of tests on  $x$ , then  $\langle \text{Maple} \rangle = 60210$ ,  $\langle \text{Mathematica} \rangle = 41870$ ,  $\langle \pi \rangle = 40220$ .
- (ii) Quantum strings pass the Borel normality test only for “much larger numbers” of counts ( $\langle \text{Quantis} \rangle = 207200$ ,  $\langle \text{Vienna} \rangle = 337100$ ),

As a result, the Borel normality test detects and identifies statistically significant differences between all pairs of computable and incomputable sources of “randomness.”

### 2. Test based on Shannon’s information theory

The results of the Kolmogorov-Smirnov test are presented in Table VII. No significant differences are detected. The descriptive statistics data for the results of this test indicates almost identical distributions corresponding to the five sources.

### 3. Tests based on algorithmic information theory

The results of the Shapiro-Wilk test are presented in Table VIII. Since there is no clear pattern of normality for the data, the application of Welch’s  $t$ -test is not appropriate.

The results of the Kolmogorov-Smirnov test associated with the “book-stack” tests are enumerated in Table IX. Statistically significant differences are identified for Quantis *versus* Mathematica and  $\pi$ .

TABLE VII. Kolmogorov-Smirnov test for Shannon’s information theory tests.

Kolmogorov-Smirnov test	$p$ -values	Mathematica	Quantis	Vienna	$\pi$
Maple		0.7870	0.7870	0.7870	0.1678
Mathematica			0.7870	0.4175	0.0525
Quantis				0.4175	0.1678
Vienna					0.4175

TABLE VIII. Shapiro-Wilk test for Shannon’s information theory tests.

Shapiro-Wilk test	Maple	Mathematica	Quantis	Vienna	$\pi$
$p$ -value	0.1962	<b>0.0189</b>	<b>0.0345</b>	0.3790	0.8774

As more compression is a symptom of less randomness, the corresponding ranking of samples is as follows:  $\langle \text{Quantis} \rangle = 89988.9 > \langle \text{Vienna} \rangle = 53863.8 > \langle \text{Maple} \rangle = 53411.6 > \langle \pi \rangle = 41277.5 > \langle \text{Mathematica} \rangle = 27938.3$ .

The Shapiro-Wilk tests results are presented in Table X.

Since normality is not rejected for any string, we apply the Welch’s  $t$ -test for the comparison of means. The results are enumerated in Table XI. Significant differences between the means are identified for the following sources: (i) Quantis *versus* all other sources (Maple, Mathematica, Vienna,  $\pi$ ); and (ii) Vienna *versus* Mathematica and Maple (as already mentioned).

The Kolmogorov-Smirnov test results are presented in Table XII, where no significant differ-

TABLE IX. Kolmogorov-Smirnov test for the “book-stack” tests.

Kolmogorov-Smirnov test	$p$ -values	Mathematica	Quantis	Vienna	$\pi$
Maple		0.4175	0.1678	0.9945	0.4175
Mathematica			<b>0.0021</b>	0.1678	0.4175
Quantis				0.1678	<b>0.0123</b>
Vienna					0.4175

TABLE X. Shapiro-Wilk test for the “book-stack” tests.

Shapiro-Wilk test	Maple	Mathematica	Quantis	Vienna	$\pi$
<i>p</i> -value	0.7880	0.4819	0.7239	0.8146	0.5172

TABLE XI. Welch’s *t*-test for the “book-stack” tests.

<i>p</i> -value	Mathematica	Quantis	Vienna	$\pi$
Maple	0.0535	<b>0.0436</b>	0.974	0.3412
Mathematica		<b>0.0009</b>	<b>0.0283</b>	0.1551
Quantis			<b>0.0368</b>	<b>0.0054</b>
Vienna				0.2690

ences are detected. The Shapiro-Wilk test results are presented in Table XIII. Since there is no clear pattern of normality for the data, the application of Welch’s *t*-test is not appropriate.

#### 4. Test based on random walks

The Kolmogorov-Smirnov test results are presented in Table XIV.

Statistically significant differences are identified for: (i) Quantis *versus* all other sources (Maple, Mathematica, Vienna and  $\pi$ ); (ii) Vienna *versus* Mathematica, Vienna (as already mentioned) and  $\pi$ ; and (iii) Maple *versus*  $\pi$ .

TABLE XII. Kolmogorov-Smirnov test for the algorithmic information theory tests.

Kolmogorov-Smirnov test	<i>p</i> -values	Mathematica	Quantis	Vienna	$\pi$
Maple		0.7591	0.4005	0.7591	0.7591
Mathematica			0.7591	0.7591	0.7591
Quantis				0.4005	0.7591
Vienna					0.9883

TABLE XIII. Shapiro-Wilk test for the algorithmic information theory tests.

Shapiro-Wilk test	Maple	Mathematica	Quantis	Vienna	$\pi$
<i>p</i> -value	0.0696	<b>0.0363</b>	0.4378	0.6963	0.4315

TABLE XIV. Kolmogorov-Smirnov test for the random walk tests.

Kolmogorov-Smirnov test	<i>p</i> -values	Mathematica	Quantis	Vienna	$\pi$
Mathematica		0.1678	<b>0.0123</b>	0.4175	0.0525
Quantis			$< 10^{-4}$	<b>0.0021</b>	0.1678
Vienna				0.0525	$< 10^{-4}$
$\pi$					<b>0.0002</b>

Note that quantum strings move farther away from the starting point than the pseudorandom strings; i.e.,  $\langle \text{Vienna} \rangle > \langle \text{Quantis} \rangle > \langle \text{Maple} \rangle > \langle \text{Mathematica} \rangle > \langle \pi \rangle$ .

It was quite natural to double-check the conclusion “Quantis and Vienna don’t exhibit significant difference.” Hence we run the Shapiro-Wilk test which concludes that normality is not rejected; cf. Table XV.

Next, we apply the Welch’s *t*-test for the comparison of means. The results are given in Table XVI. Significant differences between the means are identified for the following sources: (i) Quantis *versus* all other sources (Maple, Quantis, Vienna,  $\pi$ ); (ii) Vienna *versus* Mathematica), Quantis (as already mentioned) and  $\pi$ ; (iii) Maple *versus*  $\pi$ .

TABLE XV. Shapiro-Wilk test for the random walk tests.

Shapiro-Wilk test	Maple	Mathematica	Quantis	Vienna	$\pi$
<i>p</i> -value	0.2006	0.9268	0.5464	0.8888	0.9577

TABLE XVI. Welch’s  $t$ -tests for the random walk tests.

$p$ -value	Mathematica	Quantis	Vienna	$\pi$
Maple	0.06961	<b>0.0013</b>	0.1409	<b>0.0119</b>
Mathematica		$< 10^{-4}$	<b>0.0007</b>	<b>0.0435</b>
Quantis			<b>0.0143</b>	$< 10^{-4}$
Vienna				<b>0.0001</b>

#### IV. CONCLUSIONS

Our aim was to experimentally study the possibility of distinguishing between quantum sources of randomness—recently proved to be theoretically incomputable—and some well-known computable sources of pseudo-randomness. The experimental approach is based on algorithmic information theory which provides characterizations of algorithmic random sequences in terms of the degrees of randomness of their finite prefixes. In this theory the degree of incompressibility of a string is measured with the prefix-complexity, which, unfortunately, is incomputable. Fortunately, there are computable, but weaker properties than incompressibility which can be tested on prefixes. Of course, such a property is necessary but not sufficient, so the (degree of) absence of the property is significant.

We have performed tests of randomness on pseudo-random strings (finite sequences) of length  $2^{32}$  generated with software (Mathematica, Maple), which are cyclic (so, strongly computable), the bits of  $\pi$ , which is computable, but not cyclic, and strings produced by quantum measurements (with the commercial device Quantis and by the Vienna IQOQI group).

It is important to emphasize that our aim was to find tests capable of distinguishing computable from incomputable sources of “randomness” by examining (long, but) finite prefixes of infinite sequences. Such differences are guaranteed to exist by the result in Ref [125], but, because computability is an asymptotic property, there was no guarantee that finite tests can “pick” them in the prefixes we have analyzed [152].

With these *privisos*, our empirical randomness tests indicate quantitative differences between computable and incomputable sources of “randomness;” more specifically:

- (i) pseudo-random strings perform very well on Borel normality—in fact, too well (some over-

estimate by more than 2% of length), while the Vienna strings—which have not been post-processed—indicate deviations from Borel normality for test strings of small length (up to length 4);

- (ii) in computing Shannon’s entropy for our sequences we observe that the average seems to be the same for all sources. However, the Vienna sources clearly show a much flatter “Bell curve” around its median; the Quantis results are somewhat peculiar in that the median is clearly not centered within the 50% percentile of the entropies (indicating a skewed Bell curve) and the Mathematica sequences have a few outliers with large entropy;
- (iii) in the random walk test quantum random sources (both Vienna and Quantis) seem to move farther away from the starting point than the pseudo-generators.
- (iv) the test based on the correctness of probabilistic tests of primality is more “utilitarian,” as the metric reflects the length of the sample “random” string necessary for the Solovay-Strassen algorithm to reach the correct answer; overall, quantum random generators appear to be different from pseudo-random generators; with the Vienna strings emerging as the clear outlier (in all tests with various degrees of confidence);
- (v) the behavior of  $\pi$  (computable, but not cyclic) is interesting: in tests 1, 4 and 5 the results are closer to Mathematica and Maple, in tests 2 and 3 the results for  $\pi$  stands out (above) of all others in the direction of possibly being “more” random (according to these test metrics).

The statistical analysis of the randomness tests shows that the Borel normality test is the best test (from our collection) for detecting and differentiating between the computable and incomputable random sources; the random walk test and the “book-stack” follow in efficiency. The Shannon test and the test based on probabilistic primality behavior [128] do not produce statistically significant results. In the first case the reason may come from the fact that averages are the same for all samples. In the second case the reason may be due to the fact that the test is based solely on the behavior of algorithmic random strings and not on a specific property of randomness.

The pair of tests based on Borel normality and random walks seem to address complimentary properties helping to distinguish well between computable and incomputable sources of “randomness.” Pseudo-random strings perform better than quantum strings for the Borel normality test. One could speculate that pseudo-randomness incorporates the “human” perception of randomness, which is strongly associated with uniform distribution; in contrast, quantum randomness has no



such bias. Quantum random bits tend to take a longer time to reach “uniform distribution”—which is an asymptotical property—than pseudo-random strings.

Our analysis indicate normality of the (finite) quantum sequences for longer test strings, but violations of normality for a few small length test strings (up to length 4). Notice that for finite sequences of quantum or other origin, normality needs not be satisfied for all test strings; hence the derivations cannot be taken as a clear signal of a violation of Borel normality stemming, say, from a lack of independence. With these caveats, a conceivable (speculative and by no means necessary) physical explanation of this violation of normality for test strings of small length would be that, due to photon (Bose-Einstein) statistics and the Hanbury-Brown-Twiss effect (“photon bunching;” i.e., the tendency of photons to arrive in identical states), independence and thus Borel normality might be violated for “small” groups of data. In this line of thought, for larger sequences a sort of “late randomness” becomes visible, as the short-term correlations disappear in time. In contrast, for the random walk test, which addresses a global type of behaviour rather than a local one, quantum strings perform better: they tend to move farther away from the starting point.

A few more caveats are in order. As expected, our results indicate some tendencies only. As this is a first attempt to experimentally distinguish computable from incomputable sources of “randomness,” much more work is necessary to understand those differences. New tests should be designed to reflect the asymptotic differences. We may work with longer strings of bits to trespass the cyclicity of the pseudo-random generators [153]. We suggest that there may be different types of “quantum randomness” corresponding to different forms of quantum indeterminism (e.g., entanglement, Bell’s theorem, Kochen-Specker theorem). Finally, our experimental results clearly cannot, and do not aim, to “prove” in any formal way the superiority of quantum random generators over the best pseudo-random ones for practical applications; the only superiority is asymptotic, and resides in the differences between computable and incomputable sources proven in Ref [125].

## **ACKNOWLEDGEMENTS**

We are grateful to Thomas Jennewein and Anton Zeilinger for providing us with the quantum random bits produced at the University of Vienna by the Vienna IQOQI group, for the description of their method, critical comments and interest in this research.

We thank: a) Alastair Abbott, Hector Zenil and Boris Ryabko for interesting comments, b)

Ulrich Speidel for his tests for which some partial results have been reported in our extended paper [136], c) Stefan Wegenkittl for critical comments of various drafts of this paper and his suggestions to exclude some tests.

Cristian Calude gratefully acknowledges the support of the Hood Foundation (Fellowship Grant 2008–2009) and the Technical University of Vienna (where his work was done during his visits in 2008 and 2009). Karl Svozil gratefully acknowledges support of the Centre for Discrete Mathematics and Theoretical Computer Science (CDMTCS) at the University of Auckland, as well as of the Ausseninstitut of the Vienna University of Technology.

- 
- [1] P. Frank, *Das Kausalgesetz und seine Grenzen* (Springer, Vienna, 1932), English translation in Ref. [154].
- [2] H. Poincaré, *Wissenschaft und Hypothese* (Teubner, Leipzig, 1914).
- [3] F. Diacu, “The Solution of the N-body Problem,” *The Mathematical Intelligencer* **18**, 66–70 (1996).  
<http://dx.doi.org/10.1007/BF03024313>
- [4] K. E. Sundman, “Memoire sur le problème de trois corps,” *Acta Mathematica* **36**, 105–179 (1912).
- [5] Q. D. Wang, “The global solution of the  $N$ -body problem,” *Celestial Mechanics* **50**, 73–88 (1991).  
<http://dx.doi.org/10.1007/BF00048987>
- [6] Q. D. Wang, “Power Series Solutions and Integral Manifold of the n-body Problem,” *Regular & Chaotic Dynamics* **6**, 433–442 (2001).  
<http://dx.doi.org/10.1070/RD2001v006n04ABEH000187>
- [7] J.-P. Eckmann and D. Ruelle, “Ergodic theory of chaos and strange attractors,” *Reviews of Modern Physics* **57**, 617–656 (1985).  
<http://dx.doi.org/10.1103/RevModPhys.57.617>
- [8] F. Diacu and P. Holmes, *Celestial Encounters - the Origins of Chaos and Stability* (Princeton University Press, Princeton, 1996).
- [9] M. Born, “Ist die klassische Mechanik tatsächlich deterministisch?” *Physikalische Blätter* **11**, 49–54 (1955), English translation “Is classical mechanics in fact deterministic?” Reprinted in Ref. [155, p. 78-83].
- [10] Recall Einstein’s *dictum* in a letter to Born, dated December 12th, 1926 [155, p. 113], “In any case I am convinced that he [[the Old One]] does not throw dice.” (In German: “Jedenfalls bin

ich überzeugt, dass der [[Alte]] nicht würfelt.”).

- [11] W. Pauli, “Wahrscheinlichkeit und Physik,” *Dialectica* **8**, 112–124 (1954), English translation in Ref. [156, pp. 43-48].  
<http://dx.doi.org/10.1111/j.1746-8361.1954.tb01125.x>
- [12] A. Zeilinger, “The message of the quantum,” *Nature* **438**, 743 (2005).  
<http://dx.doi.org/10.1038/438743a>
- [13] G. J. Chaitin and J. T. Schwartz, “A note on monte carlo primality tests and algorithmic information theory,” *Communications on Pure and Applied Mathematics* **31**, 521–527 (1978).  
<http://dx.doi.org/10.1002/cpa.3160310407>
- [14] A. Granville, “Primality testing and Carmichael numbers,” *Notices of the American Mathematical Society* **39**, 696–700 (1992).  
<http://www.dms.umontreal.ca/~andrew/PDF/Notices1.pdf>
- [15] S. Mertens and H. Bauke, “Entropy of pseudo-random-number generators,” *Physical Review E* **69**, 055 702 (2004).  
<http://dx.doi.org/10.1103/PhysRevE.69.055702>
- [16] N. C. Metropolis, G. Reitweisner, and J. von Neumann, “Statistical Treatment of Values of First 2000 decimal digits of  $e$  and of  $\pi$  Calculated on the ENIAC,” *Mathematical Tables and Other Aids to Computation* **4**, 109–111 (1950), reprinted in *John von Neumann, Collected Works, (Vol. V)*, A. H. Traub, editor, MacMillan, New York, 1963, p. 765.
- [17] G. Marsaglia, “random numbers fall mainly in the planes,” *Proceedings of the National Academy of Sciences of the United States of America (PNAS)* **61**, 25–28 (1968).  
<http://www.pnas.org/content/61/1/25.full.pdf>
- [18] C. A. Pickover, “Picturing randomness on a graphics supercomputer,” *IBM Journal of Research and Development* **35**, 227–230 (1991).  
<http://www.research.ibm.com/journal/rd/351/ibmrd3501a2S.pdf>
- [19] R. L. Bowman, “Evaluating pseudo-random number generators,” *Computers & Graphics* **19**, 315–324 (1995).  
[http://dx.doi.org/10.1016/0097-8493\(94\)00158-U](http://dx.doi.org/10.1016/0097-8493(94)00158-U)
- [20] J. von Neumann, “Various Techniques Used in Connection With Random Digits,” *National Bureau of Standards Applied Math Series* **12**, 36–38 (1951), reprinted in *John von Neumann, Collected Works, (Vol. V)*, A. H. Traub, editor, MacMillan, New York, 1963, p. 768–770.

- [21] P. Diaconis, S. Holmes, and R. Montgomery, “Dynamical Bias in the Coin Toss,” *SIAM Review* **49**, 211–235 (2007).  
<http://dx.doi.org/10.1137/S0036144504446436>
- [22] C. S. Wallace, “Physically random generator,” *Computer Systems Science & Engineering* **5**, 82–88 (1990).
- [23] C. H. Vincent, “The generation of truly random binary numbers,” *Journal of Physics E: Scientific Instruments* **3**, 594–598 (1970), corrigendum in Ref. [157].  
<http://dx.doi.org/10.1088/0022-3735/3/8/303>
- [24] G. B. Agnew, “Random sources for cryptographic systems,” in *Advances in Cryptology - EURO-CRYPT’87*, A. Adamatzky, ed. (Springer, Berlin, 1987), pp. 77–82.  
<http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/E87/77.PDF>
- [25] Aware Electronics Corp.  
<http://www.aw-el.com>
- [26] Araneus Information Systems Oy, Araneus Alea I True Random Number Generator.  
<http://www.araneus.fi/products-alea-eng.html>
- [27] ComScire - Quantum World Corp.  
<http://www.comscire.com>
- [28] LavaRnd Random Number Generator.  
<http://lavarnd.org>
- [29] M. Stipčević and B. M. Rogina, “Quantum random number generator based on photonic emission in semiconductors,” *Review of Scientific Instruments* **78**, 045 104 (2007).  
<http://dx.doi.org/10.1063/1.2720728>
- [30] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, “A high speed, postprocessing free, quantum random number generator,” *Applied Physics Letters* **93**, 031 109 (2008).  
<http://dx.doi.org/10.1063/1.2961000>
- [31] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, “Photon arrival time quantum random number generation,” *Journal of Modern Optics* **56**, 516–516 (2009).  
<http://dx.doi.org/10.1080/09500340802553244>
- [32] H.-Q. Ma, Y. Xie, and L.-A. Wu, “Random number generation based on the time of arrival of single photons,” *Applied Optics* **44**, 7760–7763 (2005).  
<http://dx.doi.org/10.1364/AO.44.007760>

- [33] The RAND Corporation, *A Million Random Digits with 100,000 Normal Deviates Free Press Publishers* (Knolls Atomic Power Lab. Report KAPL-3147, Glencoe, Illinois, 1955), the data digits are obtainable *via* [http://www.rand.org/pubs/monograph\\_reports/2005/digits.txt.zip](http://www.rand.org/pubs/monograph_reports/2005/digits.txt.zip), the introduction *via* [http://www.rand.org/pubs/monograph\\_reports/MR1418/index2.html](http://www.rand.org/pubs/monograph_reports/MR1418/index2.html).  
[http://www.rand.org/pubs/monograph\\_reports/MR1418/](http://www.rand.org/pubs/monograph_reports/MR1418/)
- [34] According to The RAND Corporation’s disclosure, “The random digits in this book were produced by re-randomization of a basic table generated by an electronic roulette wheel. Briefly, a random frequency pulse source, providing on the average about 100,000 pulses per second, was gated about once per second by a constant frequency pulse. Pulse standardization circuits passed the pulses through a 5-place binary counter. In principle the machine was a 32-place roulette wheel which made, on the average, about 3000 revolutions per trial and produced one number per second. A binary-to-decimal converter was used which converted 20 of the 32 numbers (the other twelve were discarded) and retained only the final digit of two-digit numbers; this final digit was fed into an IBM punch to produce finally a punched card table of random digits.”.
- [35] R. J. Cook and H. J. Kimble, “Possibility of Direct Observation of Quantum Jumps,” *Physical Review Letters* **54**, 1023–1026 (1985).  
<http://dx.doi.org/10.1103/PhysRevLett.54.1023>
- [36] T. Erber and S. Putterman, “Randomness of quantum mechanics: nature’s ultimate cryptogram?” *Nature* **318**, 41–43 (1985).  
<http://dx.doi.org/10.1038/318041a0>
- [37] T. Erber, “Testing the Randomness of Quantum Mechanics: Nature’s Ultimate Cryptogram?” in *Annals of the New York Academy of Sciences. Volume 755 Fundamental Problems in Quantum Theory*, D. M. Greenberger and A. Zeilinger, eds. (Springer, Berlin, Heidelberg, New York, 1995), Vol. 755, pp. 748–756.  
<http://dx.doi.org/10.1111/j.1749-6632.1995.tb39016.x>
- [38] P. L. Knight, R. Loudon, and D. T. Pegg, “Quantum jumps and atomic cryptograms,” *Nature* **323**, 608–609 (1986).  
<http://dx.doi.org/10.1038/323608a0>
- [39] H. Schmidt, “Quantum-Mechanical Random-Number Generator,” *Journal of Applied Physics* **41**, 462–468 (1970).  
<http://dx.doi.org/10.1063/1.1658698>

- [40] J. Walker, “HotBits Hardware,” (1986-2009).  
<http://www.fourmilab.ch/hotbits/hardware3.html>
- [41] M. Stipčević, “Fast nondeterministic random bit generator based on weakly correlated physical events,” *Review of Scientific Instruments* **75**, 4442–4449 (2004).  
<http://dx.doi.org/10.1063/1.1809295>
- [42] K. Svozil, “The quantum coin toss—Testing microphysical undecidability,” *Physics Letters A* **143**, 433–437 (1990).  
[http://dx.doi.org/10.1016/0375-9601\(90\)90408-G](http://dx.doi.org/10.1016/0375-9601(90)90408-G)
- [43] J. G. Rarity, M. P. C. Owens, and P. R. Tapster, “Quantum Random-number Generation and Key Sharing,” *Journal of Modern Optics* **41**, 2435–2444 (1994).  
<http://dx.doi.org/10.1080/09500349414552281>
- [44] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, “A Fast and Compact Quantum Random Number Generator,” *Review of Scientific Instruments* **71**, 1675–1680 (2000).  
<http://dx.doi.org/10.1063/1.1150518>
- [45] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, “Optical quantum random number generator,” *Journal of Modern Optics* **47**, 595–598 (2000).  
<http://dx.doi.org/10.1080/095003400147908>
- [46] M. Hai-Qiang, W. Su-Mei, Z. Da, C. Jun-Tao, J. Ling-Ling, H. Yan-Xue, and W. Ling-An, “A Random Number Generator Based on Quantum Entangled Photon Pairs,” *Chinese Physics Letters* **21**, 1961–1964 (2004).  
<http://dx.doi.org/10.1088/0256-307X/21/10/027>
- [47] P. X. Wang, G. L. Long, and Y. S. Li, “Scheme for a quantum random number generator,” *Journal of Applied Physics* **100**, 056 107 (2006).  
<http://dx.doi.org/10.1063/1.2338830>
- [48] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, “Secure self-calibrating quantum random-bit generator,” *Physical Review A (Atomic, Molecular, and Optical Physics)* **75**, 032 334 (2007).  
<http://dx.doi.org/10.1103/PhysRevA.75.032334>
- [49] K. Svozil, “Three criteria for quantum random-number generators based on beam splitters,” *Physical Review A (Atomic, Molecular, and Optical Physics)* **79**, 054 306 (2009).  
<http://dx.doi.org/10.1103/PhysRevA.79.054306>

- [50] O. Kwon, Y.-W. Cho, and Y.-H. Kim, “Quantum random number generator using photon-number path entanglement,” *Applied Optics* **48**, 1774–1778 (2009).  
<http://dx.doi.org/10.1364/AO.48.001774>
- [51] M. Jammer, *The Conceptual Development of Quantum Mechanics. 2nd edition. The History of Modern Physics, 1800-1950; v. 12* (American Institute of Physics, New York, 1989).
- [52] M. Jammer, *The Philosophy of Quantum Mechanics* (John Wiley & Sons, New York, 1974).
- [53] R. P. Feynman, *The Character of Physical Law* (MIT Press, Cambridge, MA, 1965).
- [54] C. A. Fuchs and A. Peres, “Quantum theory needs no ‘Interpretation’,” *Physics Today* **53**, 70–71 (2000), further discussions of and reactions to the article can be found in the September issue of *Physics Today*, *53*, 11-14 (2000).  
<http://www.aip.org/web2/aiphome/pt/vol-53/iss-9/p11.html> and <http://www.aip.org/web2/aiphome/pt/vol-53/iss-9/p14>
- [55] J. Clauser, “Early History of Bell’s Theorem,” in *Quantum (Un)speakables. From Bell to Quantum Information* (Springer, Berlin, 2002), pp. 61–96.
- [56] M. Born, “Zur Quantenmechanik der Stoßvorgänge,” *Zeitschrift für Physik* **37**, 863–867 (1926).  
<http://dx.doi.org/10.1007/BF01397477>
- [57] M. Born, “Quantenmechanik der Stoßvorgänge,” *Zeitschrift für Physik* **38**, 803–827 (1926).  
<http://dx.doi.org/10.1007/BF01397184>
- [58] W. Pauli, “Die allgemeinen Prinzipien der Wellenmechanik,” in *Handbuch der Physik. Band V, Teil 1. Prinzipien der Quantentheorie I*, S. Flügge, ed. (Springer, Berlin, Göttingen and Heidelberg, 1958), pp. 1–168.
- [59] A. Peres, “Unperformed experiments have no results,” *American Journal of Physics* **46**, 745–747 (1978).  
<http://dx.doi.org/10.1119/1.11393>
- [60] N. D. Mermin, “Hidden variables and the two theorems of John Bell,” *Reviews of Modern Physics* **65**, 803–815 (1993).  
<http://dx.doi.org/10.1103/RevModPhys.65.803>
- [61] J. A. Wheeler and W. H. Zurek, *Quantum Theory and Measurement* (Princeton University Press, Princeton, 1983).
- [62] “Vom Standpunkt unserer Quantenmechanik gibt es keine Größe, die im *Einzelfalle* den Effekts eines Stoßes kausal festlegt; aber auch in der Erfahrung haben wir keinen Anhaltspunkt dafür, daß es innere Eigenschaften der Atome gibt, die einen bestimmten Stoßerfolg bedingen. Sollen wir hoffen,

später solche Eigenschaften [...] zu entdecken und im Einzelfalle zu bestimmen? Oder sollen wir glauben, dass die Übereinstimmung von Theorie und Erfahrung in der Unfähigkeit, Bedingungen für den kausalen Ablauf anzugeben, eine prästabilisierte Harmonie ist, die auf der Nichtexistenz solcher Bedingungen beruht? Ich selber neige dazu, die Determiniertheit in der atomaren Welt aufzugeben.”

- .
- [63] “Die Bewegung der Partikel folgt Wahrscheinlichkeitsgesetzen, die Wahrscheinlichkeit selbst aber breitet sich im Einklang mit dem Kausalgesetz aus. [Das heißt, daß die Kenntnis des Zustandes in allen Punkten in einem Augenblick die Verteilung des Zustandes zu allen späteren Zeiten festlegt.]”
- .
- [64] N. D. Mermin, *Quantum Computer Science* (Cambridge University Press, Cambridge, 2007).  
<http://people.ccmr.cornell.edu/~mermin/qcomp/CS483.html>
- [65] K. Svozil, “Contexts in quantum, classical and partition logic,” in *Handbook of Quantum Logic and Quantum Structures*, K. Engesser, D. M. Gabbay, and D. Lehmann, eds. (Elsevier, Amsterdam, 2009), pp. 551–586.  
<http://arxiv.org/abs/quant-ph/0609209>
- [66] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Springer, Berlin, 1932), English translation in Ref. [158].
- [67] S. Kochen and E. P. Specker, “The Problem of Hidden Variables in Quantum Mechanics,” *Journal of Mathematics and Mechanics* (now *Indiana University Mathematics Journal*) **17**, 59–87 (1967), reprinted in Ref. [159, pp. 235–263].  
<http://dx.doi.org/10.1512/iumj.1968.17.17004>
- [68] M. A. Neumark, “Principles of quantum theory,” in *Sowjetische Arbeiten zur Funktionalanalysis. Beiheft zur Sowjetwissenschaft*, K. Matthes, ed. (Gesellschaft für Deutsch-Sowjetische Freundschaft, Berlin, 1954), Vol. 44, pp. 195–273.
- [69] P. R. Halmos, *Finite-dimensional vector spaces* (Springer, New York, Heidelberg, Berlin, 1974).
- [70] T. J. Herzog, P. G. Kwiat, H. Weinfurter, and A. Zeilinger, “Complementarity and the quantum eraser,” *Physical Review Letters* **75**, 3034–3037 (1995).  
<http://dx.doi.org/10.1103/PhysRevLett.75.3034>
- [71] D. M. Greenberger and A. YaSin, ““Haunted” measurements in quantum theory,” *Foundation of Physics* **19**, 679–704 (1989).  
<http://dx.doi.org/10.1007/BF00731905>



- [72] S. Wiesner, “Conjugate coding,” *SIGACT News* **15**, 78–88 (1983).  
<http://dx.doi.org/10.1145/1008908.1008920>
- [73] See also the later patents at Refs. [160, 161], as well as at Refs. [162, 163].
- [74] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, “Violation of Bell’s Inequality under Strict Einstein Locality Conditions,” *Phys. Rev. Lett.* **81**, 5039–5043 (1998).  
<http://dx.doi.org/10.1103/PhysRevLett.81.5039>
- [75] F. D. Murnaghan, *The Unitary and Rotation Groups* (Spartan Books, Washington, D.C., 1962).
- [76] Z. Ou, C. Hong, and L. Mandel, “Relation between input and output states for a beam splitter,” *Optics Communications* **63**, 118–122 (1987).  
[http://dx.doi.org/10.1016/0030-4018\(87\)90271-9](http://dx.doi.org/10.1016/0030-4018(87)90271-9)
- [77] D. M. Greenberger, M. A. Horne, and A. Zeilinger, “Multiparticle interferometry and the superposition principle,” *Physics Today* **46**, 22–29 (1993).
- [78] A. Zeilinger, “General properties of lossless beam splitters in interferometry,” *American Journal of Physics* **49**, 882–883 (1981).  
<http://dx.doi.org/10.1119/1.12387>
- [79] K. Svozil, “Noncontextuality in multipartite entanglement,” *J. Phys. A: Math. Gen.* **38**, 5781–5798 (2005).  
<http://dx.doi.org/10.1088/0305-4470/38/25/013>
- [80] “To cite a human example, for simplicity, in tossing a coin it is probably easier to make two consecutive tosses independent than to toss heads with probability exactly one-half. If independence of successive tosses is assumed, we can reconstruct a 50–50 chance out of even a badly biased coin by tossing twice. If we get heads-heads or tails-tails, we reject the tosses and try again. If we get heads-tails (or tails-heads), we accept the result as heads (or tails).”
- [81] P. Elias, “The Efficient Construction of an Unbiased Random Sequence,” *Ann. Math. Statist.* **43**, 865–870 (1972).  
<http://dx.doi.org/10.1214/aoms/1177692552>
- [82] Y. Peres, “Iterating Von Neumann’s procedure for extracting random bits,” *The Annals of Statistics* **20**, 590–597 (1992).  
<http://www.jstor.org/stable/2242181>
- [83] M. Dichtl, “Bad and Good Ways of Post-processing Biased Physical Random Numbers,” in *Fast Software Encryption. Lecture Notes in Computer Science Volume 4593/2007*, A. Biryukov, ed. (Springer,

- Berlin and Heidelberg, 2007), pp. 137–152, 14th International Workshop, FSE 2007, Luxembourg, Luxembourg, March 26-28, 2007, Revised Selected Papers.  
[http://dx.doi.org/10.1007/978-3-540-74619-5\\_9](http://dx.doi.org/10.1007/978-3-540-74619-5_9)
- [84] P. Lacharme, “Post-Processing Functions for a Biased Physical Random Number Generator,” in *Fast Software Encryption. Lecture Notes in Computer Science Volume 5086/2008*, K. Nyberg, ed. (Springer, Berlin and Heidelberg, 2008), pp. 334–342, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers.  
[http://dx.doi.org/10.1007/978-3-540-71039-4\\_21](http://dx.doi.org/10.1007/978-3-540-71039-4_21)
- [85] J. C. Garrison and R. Y. Chiao, *Quantum Optics* (Oxford, Oxford, 2008).
- [86] C. Gerry and P. L. Knight, *Introductory Quantum Optics* (Cambridge University Press, Cambridge, UK, 2005).
- [87] E. Schrödinger, “Die gegenwärtige Situation in der Quantenmechanik,” *Naturwissenschaften* **23**, 807–812, 823–828, 844–849 (1935), English translation in Ref. [164] and in Ref. [61, pp. 152-167].  
<http://dx.doi.org/10.1007/BF01491891>,  
<http://dx.doi.org/10.1007/BF01491914>,  
<http://dx.doi.org/10.1007/BF01491987>
- [88] In its *White Paper on Random Numbers Generation using Quantum Physics* [132], *id Quantique* on p. 7 (in the caption to Fig. 1) announces that its *Quantis* device uses a light emitting diode, while at the same time (top of p. 7) pointing out that the monitoring of a Zener diode is problematic: “Formally the evolution of these generators is not random, but just very complex. One could say that determinism is hidden behind complexity.”.
- [89] E. F. Moore, “Gedanken-Experiments on Sequential Machines,” in *Automata Studies*, C. E. Shannon and J. McCarthy, eds. (Princeton University Press, Princeton, 1956), pp. 129–153.
- [90] R. Wright, “Generalized urn models,” *Foundations of Physics* **20**, 881–903 (1990).  
<http://dx.doi.org/10.1007/BF01889696>
- [91] K. Svozil, “Logical equivalence between generalized urn models and finite automata,” *International Journal of Theoretical Physics* **44**, 745–754 (2005).  
<http://dx.doi.org/10.1007/s10773-005-7052-0>
- [92] K. Svozil, “Staging quantum cryptography with chocolate balls,” *American Journal of Physics* **74**, 800–803 (2006).  
<http://dx.doi.org/10.1119/1.2205879>

- [93] B. Misra and E. C. G. Sudarshan, “The Zeno’s paradox in quantum theory,” *Journal of Mathematical Physics* **18**, 756–763 (1977).  
<http://dx.doi.org/10.1063/1.523304>
- [94] W. Heisenberg, “Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik,” *Zeitschrift für Physik* **43**, 172–198 (1927), english translation in Ref. [61, pp. 62-84].  
<http://dx.doi.org/10.1007/BF01397280>
- [95] J. von Neumann, “Wahrscheinlichkeitstheoretischer Aufbau der Quantenmechanik. (German) [Probabilistic structure of quantum mechanics],” *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen* **1**, 245–272 (1927), reprinted in [165, Paper 10].  
<http://www.digizeitschriften.de/main/dms/img/?IDDOC=465854>
- [96] P. A. M. Dirac, *The Principles of Quantum Mechanics* (Oxford University Press, Oxford, 1930).
- [97] “Bei der Unbestimmtheit einer Eigenschaft eines Systems bei einer bestimmten Anordnung (bei einem bestimmten Zustand eines Systems) vernichtet jeder Versuch, die betreffende Eigenschaft zu messen, (mindestens teilweise) den Einfluß der früheren Kenntnisse vom System auf die (eventuell statistischen) Aussagen über spätere mögliche Messungsergebnisse. [[...]] So müssen, um den Ort eines Teilchens zu bestimmen und um seinen Impuls zu bestimmen, *einander ausschließende Versuchsanordnungen benutzt werden*. [[...]] Die Beeinflussung des Systems durch den Messapparat für den Impuls (Ort) ist eine solche, daß innerhalb der durch die Ungenauigkeitsrelationen gegebenen Grenzen die Benutzbarkeit der früheren Orts- (Impuls-) Kenntnis für die Voraussagbarkeit der Ergebnisse späterer Orts- (Impuls-) Messungen verlorengegangen ist. Wenn aus diesem Grunde die Benutzbarkeit *eines* klassischen Begriffes in einem ausschließenden Verhältnis zu einem *anderen* steht, nennen wir diese beiden Begriffe (z.B. Orts- und Impulskoordinaten eines Teilchens) mit Bohr *komplementär*. [[...]] Man wird sehen, dass diese “Komplementarität” kein Analogon in der klassischen Gastheorie besitzt, die ja auch mit statistischen Gesetzmäßigkeiten operiert. Diese Theorie enthält nämlich nicht die erst durch die Endlichkeit des Wirkungsquantums geltend werdende Aussage, daß durch Messungen an einem System die durch frühere Messungen gewonnenen Kenntnisse über das System unter Umständen notwendig verlorengehen müssen, d.h. nicht mehr verwertet werden können.” .
- [98] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?” *Physical Review* **47**, 777–780 (1935).  
<http://dx.doi.org/10.1103/PhysRev.47.777>

- [99] K. Svozil, “Quantum Scholasticism: On Quantum Contexts, Counterfactuals, and the Absurdities of Quantum Omniscience,” *Information Sciences* **179**, 535–541 (2009).  
<http://dx.doi.org/10.1016/j.ins.2008.06.012>
- [100] K. Svozil, “Are simultaneous Bell measurements possible?” *New Journal of Physics* **8**, 39 (2006).  
<http://dx.doi.org/10.1088/1367-2630/8/3/039>
- [101] A. M. Gleason, “Measures on the closed subspaces of a Hilbert space,” *Journal of Mathematics and Mechanics (now Indiana University Mathematics Journal)* **6**, 885–893 (1957).  
<http://dx.doi.org/10.1512/iumj.1957.6.56050>
- [102] I. Pitowsky, “Infinite and finite Gleason’s theorems and the logic of indeterminacy,” *Journal of Mathematical Physics* **39**, 218–228 (1998).  
<http://dx.doi.org/10.1063/1.532334>
- [103] F. Richman and D. Bridges, “A constructive proof of Gleason’s theorem,” *Journal of Functional Analysis* **162**, 287–312 (1999).  
<http://dx.doi.org/10.1006/jfan.1998.3372>
- [104] A. Dvurečenskij, *Gleason’s Theorem and Its Applications* (Kluwer Academic Publishers, Dordrecht, 1993).
- [105] J. S. Bell, “On the Einstein Podolsky Rosen paradox,” *Physics* **1**, 195–200 (1964), reprinted in Ref. [61, pp. 403-408] and in [166, pp. 14-21].
- [106] P. Heywood and M. L. G. Redhead, “Nonlocality and the Kochen-Specker Paradox,” *Foundations of Physics* **13**, 481–499 (1983).  
<http://dx.doi.org/10.1007/BF00729511>
- [107] D. M. Greenberger, M. A. Horne, and A. Zeilinger, “Going beyond Bell’s theorem,” in *Bell’s Theorem, Quantum Theory, and Conceptions of the Universe*, M. Kafatos, ed. (Kluwer Academic Publishers, Dordrecht, 1989), pp. 73–76.
- [108] E. Specker, “Die Logik nicht gleichzeitig entscheidbarer Aussagen,” *Dialectica* **14**, 239–246 (1960), reprinted in Ref. [159, pp. 175–182]; English translation: *The logic of propositions which are not simultaneously decidable*, Reprinted in Ref. [167, pp. 135-140].  
<http://dx.doi.org/10.1111/j.1746-8361.1960.tb00422.x>
- [109] N. Zierler and M. Schlessinger, “Boolean embeddings of orthomodular sets and quantum logic,” *Duke Mathematical Journal* **32**, 251–262 (1965).
- [110] V. Alda, “On 0-1 measures for projectors I,” *Aplik. mate.* **25**, 373–374 (1980).

- [111] V. Alda, “On 0-1 measures for projectors II,” *Aplik. mate.* **26**, 57–58 (1981).
- [112] F. Kamber, “Die Struktur des Aussagenkalküls in einer physikalischen Theorie,” *Nachr. Akad. Wiss. Göttingen* **10**, 103–124 (1964).
- [113] F. Kamber, “Zweiwertige Wahrscheinlichkeitsfunktionen auf orthokomplementären Verbänden,” *Mathematische Annalen* **158**, 158–196 (1965).
- [114] A. Peres, “Two simple proofs of the Kochen-Specker theorem,” *Journal of Physics A: Mathematical and General* **24**, L175–L178 (1991), reprinted in Ref. [126, pp. 186-200].  
<http://dx.doi.org/10.1088/0305-4470/24/4/003>
- [115] K. Svozil and J. Tkadlec, “Greechie diagrams, nonexistence of measures in quantum logics and Kochen–Specker type constructions,” *Journal of Mathematical Physics* **37**, 5380–5401 (1996).  
<http://dx.doi.org/10.1063/1.531710>
- [116] A. Cabello, J. M. Estebarez, and G. García-Alcaine, “Bell-Kochen-Specker theorem: A proof with 18 vectors,” *Physics Letters A* **212**, 183–187 (1996).  
[http://dx.doi.org/10.1016/0375-9601\(96\)00134-X](http://dx.doi.org/10.1016/0375-9601(96)00134-X)
- [117] A. Cabello, “Experimentally Testable State-Independent Quantum Contextuality,” *Physical Review Letters* **101**, 210401 (2008).  
<http://dx.doi.org/10.1103/PhysRevLett.101.210401>
- [118] N. Bohr, “Discussion with Einstein on epistemological problems in atomic physics,” in *Albert Einstein: Philosopher-Scientist*, P. A. Schilpp, ed. (The Library of Living Philosophers, Evanston, Ill., 1949), pp. 200–241.  
<http://www.emr.hibu.no/lars/eng/schilpp/Default.html>
- [119] J. S. Bell, “On the Problem of hidden variables in quantum mechanics,” *Reviews of Modern Physics* **38**, 447–452 (1966), reprinted in Ref. [166, pp. 1-13].  
<http://dx.doi.org/10.1103/RevModPhys.38.447>
- [120] M. Redhead, *Incompleteness, Nonlocality, and Realism: A Prolegomenon to the Philosophy of Quantum Mechanics* (Clarendon Press, Oxford, 1990).
- [121] Other schemes to circumvent the quantum value indefiniteness are through probabilities defined via paradoxical set decompositions [168, 169] or by considering certain dense subsets of scarcely inter-linked quantum contexts [170].
- [122] K. Svozil, “Proposed direct test of a certain type of noncontextuality in quantum mechanics,” *Physical Review A (Atomic, Molecular, and Optical Physics)* **80**, 040102 (2009).

- <http://dx.doi.org/10.1103/PhysRevA.80.040102>
- [123] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, “Violation of Bell’s Inequality under Strict Einstein Locality Conditions,” *Phys. Rev. Lett.* **81**, 5039–5043 (1998).  
<http://dx.doi.org/10.1103/PhysRevLett.81.5039>
- [124] A. Shimony, “Controllable and uncontrollable non-locality,” in *Proceedings of the International Symposium on the Foundations of Quantum Mechanics*, S. K. et al., ed., pp. 225–230 (1984), see also J. Jarrett, *Bell’s Theorem, Quantum Mechanics and Local Realism*, Ph. D. thesis, Univ. of Chicago, 1983; *Nous*, **18**, 569 (1984).
- [125] C. S. Calude and K. Svozil, “Quantum Randomness and Value Indefiniteness,” *Advanced Science Letters* **1**, 165–168 (2008).  
<http://www.ingentaconnect.com/content/asp/asl/2008/00000001/00000002/art00004>
- [126] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic Publishers, Dordrecht, 1993).
- [127] K. Svozil, *Quantum Logic* (Springer, Singapore, 1998).
- [128] C. Calude, *Information and Randomness—An Algorithmic Perspective* (Springer, Berlin, 2002), 2nd edn.
- [129] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Hekert, J. Dray, and S. Vo, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22* (National Institute of Standards and Technology (NIST), 2001).  
<http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22b.pdf>
- [130] “Mathematica random generator,” .  
<http://reference.wolfram.com/mathematica/tutorial/RandomNumberGeneration.html>
- [131] “Maple random generator,” .  
[http://www.maplesoft.com/applications/app\\_center\\_view.aspx?AID=2027&CID=4&SCID=9](http://www.maplesoft.com/applications/app_center_view.aspx?AID=2027&CID=4&SCID=9)
- [132] id Quantique, “The Quantis Quantum Random Number Generator,” (2001-2009).  
<http://www.idquantique.com/products/files/quantis-whitepaper.pdf>
- [133] IQOQI Group Vienna, personal communication.
- [134] Y. Kanada and D. Takahashi, “Calculation of  $\pi$  up to 4,294,960,000 decimal digits,” (1995).  
<ftp://pi.super-computing.org>
- [135] For the curious, our ten pairs of deleted digits were  $\{0, 1\}$ ,  $\{0, 5\}$ ,  $\{1, 6\}$ ,  $\{2, 3\}$ ,  $\{2, 7\}$ ,  $\{3, 8\}$ ,  $\{4, 5\}$ ,  $\{4, 9\}$ ,  $\{6, 7\}$ , and  $\{8, 9\}$ .

- [136] C. S. Calude, M. J. Dinneen, M. Dumitrescu, and K. Svozil, “How Random Is Quantum Randomness? (Extended Version),” Report CDMTCS-372, Centre for Discrete Mathematics and Theoretical Computer Science, University of Auckland, Auckland, New Zealand (2009).  
<http://www.cs.auckland.ac.nz/CDMTCS/researchreports/372crismjdkarl.pdf>
- [137] E. Borel, “Les probabilités dénombrables et leurs applications arithmétiques,” *Rendiconti del Circolo Matematico di Palermo* (1884 - 1940) **27**, 247–271 (1909).  
<http://dx.doi.org/10.1007/BF03019651>
- [138] .
- [139] C. Calude, “Borel Normality and Algorithmic Randomness,” in *Developments in Language Theory*, G. Rozenberg and A. Salomaa, eds. (World Scientific, Singapore, 1994), pp. 113–129.
- [140] A. D. Wyner, “Shannon Lecture: Typical Sequences and All That: Entropy, Pattern Matching, and Data Compression,” IEEE Information Theory Society (1994).  
<http://www.itsoc.org/people/awards-and-honors/claude-e.-shannon-award/Wyner94Shannon.pdf/view>
- [141] B. Y. Ryabko and A. I. Pestunov, ““Book stack” as a new statistical test for random numbers,” *Problemy Peredachi Informatsii* **40**, 73–78 (2004).
- [142] B. Y. Ryabko and V. A. Monarev, “Using information theory approach to randomness testing,” *J. Statist. Plann. Inference* **133**, 95–110 (2005).
- [143] R. Solovay and V. Strassen, “A Fast Monte-Carlo Test for Primality,” *SIAM Journal on Computing* **6**, 84–85 (1977), corrigendum in Ref. [171].  
<http://dx.doi.org/10.1137/0206006>
- [144] In fact, every “decent” Monte Carlo simulation algorithm in which tests are chosen according to an algorithmic random string produces a result which is not only true with high probability, but *rigorously correct* [172].
- [145] There are 1,401,644 Carmichael numbers in the interval  $[1, 10^{18}]$ .
- [146] R. G. Pinch, “The Carmichael numbers up to  $10^{16}$ ,” (1998).  
<http://arxiv.org/abs/math.NT/9803082>
- [147] R. G. Pinch, “The Carmichael numbers up to  $10^{21}$ ,” in *Proceedings of Conference on Algorithmic Number Theory 2007. TUCS General Publication No 46* pp. 129–131 (2007).  
<http://tucs.fi/publications/attachment.php?fname=G46.pdf>
- [148] W. J. Conover, *Practical Nonparametric Statistics* (John Wiley & Sons, New York, 1999).
- [149] S. S. Shapiro and M. B. Wilk, “An analysis of variance test for normality (complete samples),”

- Biometrika **52**, 591–611 (2005).  
<http://dx.doi.org/10.1093/biomet/52.3-4.591>
- [150] B. L. Welch, “The generalization of “Student’s” problem when several different population variances are involved,” *Biometrika* **34** (1947).  
<http://dx.doi.org/10.1093/biomet/34.1-2.28>
- [151] T. R. Foundation, “The R Project for Statistical Computing, Version 2.10.0,”  
<Http://www.r-project.org>.  
<http://www.r-project.org>
- [152] Many inconclusive tests have been discarded.
- [153] Borel normality obviously fails for longer strings.
- [154] P. Frank and R. S. Cohen (Editor), *The Law of Causality and its Limits (Vienna Circle Collection)* (Springer, Vienna, 1997).
- [155] M. Born, *Physics in my generation* (Springer Verlag, New York, 1969), 2nd edn.
- [156] W. Pauli, *Writings on physics and philosophy* (Springer Verlag, Berlin, New York, 1994), ed. by Charles Paul Enz and Karl von Meyenn.
- [157] C. H. Vincent, “The generation of truly random binary numbers,” *Journal of Physics E: Scientific Instruments* **3**, 832 (1970).  
<http://dx.doi.org/10.1088/0022-3735/3/10/528>
- [158] J. von Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press, Princeton, 1955).
- [159] E. Specker, *Selecta* (Birkhäuser Verlag, Basel, 1990).
- [160] W. Dultz and E. Hildebrandt, “Optical random-check generator based on the individual photon statistics at the optical beam divider. (German: Optischer Zufallsgenerator basierend auf der Einzelphotonenstatistik am optischen Strahlteiler),” (1999), patent Pub. No.: WO/1998/016008, International Application No.: PCT/EP1997/005082, Publication Date: 16.04.1998, International Filing Date: 17.09.1997, Chapter 2 Demand Filed: 23.04.1998, IPC: H03K 3/84 (2006.01).  
<http://www.wipo.int/pctdb/en/wo.jsp?wo=1998016008>
- [161] W. Dultz, G. Dultz, E. Hildebrandt, and H. Schmitzer, “Method for generating a random number on a quantum-mechanics basis and random generator. (German: Verfahren zur Erzeugung einer Zufallszahl auf quantenmechanischer Grundlage und Zufallsgenerator),” (1999), patent Pub. No.: WO/1999/066641, International Application No.: PCT/EP1999/003689, Publication Date:



- 23.12.1999, International Filing Date: 28.05.1999, IPC: G06F 7/58 (2006.01), H03K 3/84 (2006.01).  
<http://www.wipo.int/pctdb/en/wo.jsp?wo=1999066641>
- [162] G. Ribordy and O. Guinnard, “Method and apparatus for generating true random numbers by way of a quantum optics process,” (2004), patent Application number: 10/919,573, Publication number: US 2005/0071400 A1, Filing date: Aug 17, 2004, U.S. Classification 708250000, International Classification G06F001/02.  
<http://www.google.com/patents?id=eQqXAAAAEBAJ>
- [163] G. Ribordy and O. Guinnard, “Method and apparatus for generating true random numbers by way of a quantum optics process,” (2006), patent Application number: 11/422,704, Publication number: US 2007/0127718 A1, Filing date: Jun 7, 2006, U.S. Classification 380256000.  
<http://www.google.com/patents?id=BUmiAAAAEBAJ>
- [164] J. D. Trimmer, “The present situation in quantum mechanics: a translation of Schrödinger’s “cat paradox”,” *Proceedings of the American Philosophical Society* **124**, 323–338 (1980), reprinted in Ref. [61, pp. 152-167].  
<http://www.tu-harburg.de/rzt/rzt/it/QM/cat.html>
- [165] J. von Neumann, *John von Neumann: Collected Works: Volume I: Logic, Theory of Sets and Quantum Mechanics* (Pergamon, New York, NY, 1961).
- [166] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, 1987).
- [167] C. A. Hooker, *The Logico-Algebraic Approach to Quantum Mechanics. Volume I: Historical Evolution* (Reidel, Dordrecht, 1975).
- [168] I. Pitowsky, “Resolution of the Einstein-Podolsky-Rosen and Bell paradoxes,” *Physical Review Letters* **48**, 1299–1302 (1982).  
<http://dx.doi.org/10.1103/PhysRevLett.48.1299>
- [169] I. Pitowsky, “Deterministic model of spin and statistics,” *Physical Review D* **27**, 2316–2326 (1983).  
<http://dx.doi.org/10.1103/PhysRevD.27.2316>
- [170] D. A. Meyer, “Finite precision measurement nullifies the Kochen-Specker theorem,” *Physical Review Letters* **83**, 3751–3754 (1999).  
<http://dx.doi.org/10.1103/PhysRevLett.83.3751>
- [171] R. Solovay and V. Strassen, “Erratum: A Fast Monte-Carlo Test for Primality,” *SIAM Journal on Computing* **7**, 118 (1978).

<http://dx.doi.org/10.1137/0207009>

- [172] C. Calude and M. Zimand, “A relation between correctness and randomness in the computation of probabilistic algorithms,” *Internat. J. Comput. Math.* **16**, 47–53 (1984).