A Quantum Random Number Generator Certified by Entanglement and Value Indefiniteness

Alastair A. Abbott* and Cristian S. Calude†
Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand

Karl Svozil‡
Institut für Theoretische Physik, Vienna University of Technology, Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria

We present and analize a novel protocol for a quantum random number generator secured by the indeterminacy of individual quanta in an entangled state, as well as by quantum value indefiniteness.

PACS numbers: 03.65.Ta,03.65.Ud
Keywords: quantum randomness, value indefiniteness, incomputability, unbiasing

I. INTRODUCTION

In physicist, "randomness" [1] has often been perceived negatively as a disadvantage indicating an absence of control, predictability, and knowability. Only recently there seems to have emerged an understanding of random behaviour of a physical system as a valuable resource and capacity. Indeed, any system postulated to behave randomly outperforms (universal) computers and thus represents a concrete instance of actual hypercomputation.

Whether and how physical randomness could be given a precise formalization, in particular, by considering a uniform, deterministic, unitary evolution of the quantum state, appears to be a problem deeply rooted in, and related to, the quantum measurement problem [2]. In addition to foundational issues, one should keep in mind that the inevitable finiteness of the strings generated makes impossible the application of transfinite arguments often encountered in formal definitions. Even the assumption of independence of two events is questionable, since quantum mechanics does not exclude the entanglement of events inside a sufficiently large joint causal light cone. It is thus assumed that quantum systems perform "randomly" for all practical purposes [3].[4]

In what follows we propose a random number generator utilizing two nonclassical aspects of quantum mechanics. *Quantum entanglement* [5–7] ensures that the information is encoded into multipartite states [8]. Thereby it manifests itself in the joint properties of the quanta. The states and properties of single quanta remain inherently undefined and undetermined.

Under the assumption of noncontextuality, *quantum value indefiniteness* ensures the impossibility to ascribe definite elements of physical reality [9] to certain even finite (counterfactual) observables in systems with three or more mutually exclusive outcomes [10]. Quantum value definiteness occurs for complementary sets of observables. In such a regime, incomputability of the generated sequences is guaranteed by the underlying physical assumptions and principles [11].

The quantum random number generators have exploited sone of these aspects. Quantum complementarity has motivated realizations by beam splitters [12–17]. Entangled photon pairs have been used in more devices [18–20]; the latter one utilizing Boole-Bell-type inequality violations in the spirit of quantum cryptographic protocols [21, 22].

With regard to the relevance of quantum violations of Boole-Bell type inequalities to "randomness," whereas such violations may provide some indirect statistical verification of value indefiniteness (again under the assumption of noncontextuality), they fall short of providing certification of strong incomputability *via* value indefiniteness [11, 23]. The difference between violations of Boole-Bell-type inequalities *versus* Kochen-Specker-type theorems is this: In the Boole-Bell-type case, the breach of value indefiniteness needs not happen at every single particle, whereas in the Kochen-Specker-type case this must happen *for every particle* [24]. Pointedly stated, the Boole-Bell-type violation is statistical, but *not necessarily* on every quantum separately. Alas, because a Boole-Bell-type violation does not guarantee that every bit is certified by value indefiniteness, potentially such sequences containing infinite computable subsequences protected by Boole-Bell-type violations could be produced. Such criticisms seem also to hold for the statistical verification of value indefiniteness [25–27]. Thus it seems unlikely that statistical tests of the measurement outcomes alone can fully certify such a quantum random number generator.

In what follows, a proposal for a quantum random number generator previously put forward in Ref. [23], will be discussed in detail. It utilizes the singlet state of two two-state particles – e.g., photons of linear polarization – proportional to $|\Psi^-\rangle = |H_1V_2\rangle - |V_1H_2\rangle$, presumably by spontaneous parametric down-conversion in a nonlinear medium. Ideally, the two resulting entangled photons are then analyzed with respect to their linear polarization state at some directions which are exactly $\pi/4$ radians apart, symbolized by "$\oplus$" and "$\otimes$," respectively.

Due to the required four-dimensional Hilbert space, this quantum random number generator is protected by value indefiniteness. It is also protected by the individual measurements of quanta which are in an entangled state encoded to represent opposite linear polarization in all spatial directions.

* aabb009@aucklanduni.ac.nz; http://www.cs.auckland.ac.nz/~aabb009
† c.calude@auckland.ac.nz; http://www.cs.auckland.ac.nz/~cristian
‡ svozil@tuwien.ac.at; http://tph.tuwien.ac.at/~svozil

Formally, suppose that for the ith experimental run, the two outcomes are $O_i^{\oplus} \in \{0,1\}$ corresponding to $D_0^{\oplus}$ or $D_1^{\oplus}$, and $O_i^{\otimes} \in \{0,1\}$ corresponding to $D_0^{\otimes}$ or $D_1^{\otimes}$. These two outcomes $O_i^{\oplus}$ and $O_i^{\otimes}$, which themselves form two sequences of random bits, are subsequently combined by the XOR operation, which amounts to their parity, or to the addition modulo 2 (in what follows, depending on the formal context, XOR refers to either a binary function of two binary observables, or to the logical operation). Stated differently, one outcome is used as a *one time pad* to "encrypt" the other outcome, and *vice versa*. As a result, one obtains a sequence $x = x_1 x_2 \ldots x_n$ with

$$x_i = O_i^{\oplus} + O_i^{\otimes} \bmod 2. \tag{1}$$

For the XORd sequence to still be certifiably incomputable (via value indefiniteness), one must prove this certification is preserved under XORing – indeed strong incomputability itself is *not* necessarily preserved. By necessity any quantum random number generator certified by value indefiniteness must operate non-trivially in a Hilbert space of dimension $n \geq 3$. To transform the n-ary (incomputable) sequence into a binary one, a function $f : \{0,1,\ldots,n-1\} \to \{0,1,\lambda\}$ must be used (λ is the empty string); to claim certification, the strong incomputability of the bits must still be guaranteed after the application of f. This is a fundamental issue which has to be checked for existing quantum random number generators such as that in Ref. [20]; without it one cannot claim to produce truly indeterministic bits. In general incomputability itself is not preserved by f; however by consideration of the value indefiniteness of the source the certification can be seen to hold under XOR as well as when discarding bits [28].

The protocol is a good example of the fact that quantum mechanical correlations may contribute to larger systematic errors than in the classical case. As no experimental realization will attain a "perfect anti-alignment" of the polarization analyzers at angles $\pi/4$ radians apart. Only in this ideal case are the bases conjugate and the correlation function will be exactly zero. Indeed, "tuning" the angle to obtain equi-balanced sequences of zeroes and ones may be a method to properly anti-align the polarizers. However, one has to keep in mind that any such "tampering" with the raw sequence of data to achieve Borel normality (e.g. by readjustments of the experimental setup) may introduce unwanted (temporal) correlations or other bias [3].

Incidentally, the angle $\pi/4$ is one of the three points at angles 0, $\pi/4$ and $\pi/2$ in the interval $[0,\pi/2]$ in which the classical and quantum correlation functions coincide. For all other angles, there is a higher ratio of different or identical pairs than could be expected classically. Thus, ideally, the quantum random number generator could be said to operate in the "quasi classical" regime, albeit fully certified by quantum value indefiniteness.

Quantitatively, the expectation function of the sum of the two outcomes modulus 2 can be defined by averaging over the sum modulo 2 of the outcomes $O_i^0, O_i^{\theta} \in \{0,1\}$ at angle θ "apart" in the ith experiment, over a large number of experiments; i.e., $E_{\mathtt{XOR}}(\theta) = \lim_{N\to\infty}(1/N)\sum_{i=1}^{N}\left(O_i^0 + O_i^{\theta} \bmod 2\right)$. This is related to the standard correlation function, $C(\theta) = \lim_{N\to\infty}(1/N)\sum_{i=1}^{N} O_i^0 \cdot O_i^{\theta}$ by $E_{\mathtt{XOR}}(\theta) = (|C(\theta)-1|)/2$, where

$$O_i^0 \cdot O_i^{\theta} = \begin{cases} 1, & \text{if } O_i^0 = O_i^{\theta}, \\ -1, & \text{if } O_i^0 \neq O_i^{\theta}. \end{cases}$$

A detailed calculation yields the classical linear expectation function $E_{\mathtt{XOR}}^{\mathrm{cl}}(\theta) = 1 - 2\theta/\pi$, and the quantum expectation function $E_{\mathtt{XOR}}(\theta) = (1/2)(1+\cos 2\theta)$.

Thus, for angles "far apart" from $\pi/4$, the XOR operation *deteriorates* the two random signals taken from the two analyzers *separately.* The deterioration is even *greater quantum mechanically than classically,* as the entangled particles are more correlated and thus "less independent." Potentially, this could be utilized to ensure a $\pi/4$ mismatch more accurately than possible through classical means.

In what follows we analyze the output distribution of the proposed quantum random number generator and the ability to extract uniformly distributed bits from the two generated bitstrings in the presence of experimental imperfections.

We may write the generated Bell singlet state with respect the top ("$\oplus$") measurement context (this is arbitrary as the singlet is form invariant in all measurement directions) as $(1/\sqrt{2})(|01\rangle - |10\rangle)$. One ("$\otimes$") polarizer is at an angle of θ to the other one. After the beam splitters we have the state $\frac{1}{\sqrt{2}}[\cos\theta(|00\rangle - |11\rangle) - \sin\theta(|01\rangle + |10\rangle)]$, so we measure the same outcome in both contexts with probability $\cos^2\theta$ and different outcomes with probability $\sin^2\theta$.

More formally, the quantum random number generator generates two strings simultaneously, so the probability space contains pairs of strings of length n. Let $e_x^{\oplus}, e_y^{\otimes}$ for $x,y = 0,1$ be the detector efficiencies of the $D_x^{\oplus}$ and $D_y^{\otimes}$ detectors respectively. For perfect detectors, i.e $e_x^{\oplus} = e_y^{\otimes}$, we would expect a pair of bits (a,b) to be measured with probability $2^{-1}(\sin^2\theta)^{a\oplus b}(\cos^2\theta)^{1-a\oplus b}$; non-perfect detectors alter this probability depending on the values of a,b.

Let $B = \{0,1\}$, and for $x,y \in B^n$ let $d(x,y)$ be the Hamming distance between the strings x and y, i.e the number of positions at which x and y differ, and let $\#_b(x)$ be the number of bs in x.

The probability space [29] of bitstrings produced by the quantum random number generator is $(B^n \times B^n, 2^{B^n\times B^n}, P_{n^2})$, where the probability $P_{n^2} : 2^{B^n\times B^n} \to [0,1]$ is defined for all $X \subseteq B^n \times B^n$ as follows:

$$P_{n^2}(X) = \frac{1}{Z_n}\sum_{(x,y)\in X}(\sin^2\theta)^{d(x,y)}(\cos^2\theta)^{n-d(x,y)}(e_0^{\oplus})^{\#_0(x)}(e_1^{\oplus})^{\#_1(x)}(e_0^{\otimes})^{\#_0(y)}(e$$

and the term

$$\begin{aligned} Z_n &= \sum_{(x,y)\in B^n\times B^n}(\sin^2\theta)^{d(x,y)}(\cos^2\theta)^{n-d(x,y)}(e_0^{\oplus})^{\#_0(x)}(e_1^{\oplus})^{\#_1(x)}(e_0^{\otimes})^{\#_0(y)}(e_1^{\otimes}) \\ &= \left[(\sin^2\theta(e_0^{\oplus}e_1^{\otimes} + e_1^{\oplus}e_0^{\otimes}) + \cos^2\theta(e_0^{\oplus}e_0^{\otimes} + e_1^{\oplus}e_1^{\otimes})\right]^n \end{aligned}$$

ensures normalization.

We can check easily that this is indeed a valid probability space (i.e. that is satisfies the Kolmogorov axioms [30]). Note that for equal detector efficiencies we have

$$Z_n = (e^{\oplus})^n(e^{\otimes})^n \sum_{(x,y)\in B^n\times B^n}(\sin^2\theta)^{d(x,y)}(\cos^2\theta)^{n-d(x,y)} = 2^n(e^{\oplus})^n(e^{\otimes})^n,$$

hence the probability has the simplified form

$$P_{n^2}(X) = \sum_{(x,y)\in X} 2^{-n}(\sin^2\theta)^{d(x,y)}(\cos^2\theta)^{n-d(x,y)}.$$

Given that the proposed quantum random number generator produces two (potentially correlated) strings, it is worth considering the distribution of each string taken separately. Given the rotational invariance of the singlet state this should be uniformly distributed. However, because the detector efficiencies may vary in each detector, this is not, in general, the case. For every bitstring $x \in B^n$ we have

$$\begin{aligned} P_{n^2}(\{x\}\times B^n) &= \frac{1}{Z_n}\sum_{y\in B^n}(\sin^2\theta)^{d(x,y)}(\cos^2\theta)^{n-d(x,y)}(e_0^{\oplus})^{\#_0(x)}(e_1^{\oplus})^{\#_1(x)}(e_0^{\otimes})^{\#_0(y)}(e_1^{\otimes})^{\#_1(y)} \\ &= \frac{(e_0^{\oplus})^{\#_0(x)}(e_1^{\oplus})^{\#_1(x)}}{Z_n}\sum_{y\in B^n}(\sin^2\theta)^{d(x,y)}(\cos^2\theta)^{n-d(x,y)}(e_0^{\otimes})^{\#_0(y)}(e_1^{\otimes})^{\#_1(y)} \\ &= \frac{1}{Z_n}\left(e_0^{\oplus}(e_1^{\otimes}\sin^2\theta + e_0^{\otimes}\cos^2\theta)\right)^{\#_0(x)}\left(e_1^{\oplus}(e_0^{\otimes}\sin^2\theta + e_1^{\otimes}\cos^2\theta)\right)^{\#_1(x)}. \end{aligned} \tag{2}$$

We see that each bitstring taken separately appears to come from a constantly biased source where the probabilities that a bit is 0 or 1, p_0, p_1, are given by the formulae

$$p_0 = e_0^{\oplus}(e_1^{\otimes}\sin^2\theta + e_0^{\otimes}\cos^2\theta)/Z_1,\ p_1 = e_1^{\oplus}(e_0^{\otimes}\sin^2\theta + e_1^{\otimes}\cos^2\theta)/Z_1.$$

This can alternatively be viewed as the distribution obtained if we were to discard one bitstring after measurement. Note that if either $e_0^{\otimes} = e_1^{\otimes}$ or we have perfect misalignment (i.e. $\theta = \pi/4$) then the probabilities have the simpler formulae:

$$p_x = e_x^{\oplus}/(e_0^{\oplus} + e_1^{\oplus}), x \in \{0,1\}.$$

In this case, if we further have that $e_0^{\oplus} = e_1^{\oplus}$, we obtain the uniform distribution by discarding one string after measurement.

The analogous result for the symmetrical case $P_{n^2}(B^n \times \{y\})$ also holds.

If we were to discard one bitstring it is clear the other bitstring is generated independently in a statistical sense since the probability distribution source producing it is constantly biased and independent [31]. However, we would like to extend our notion of independence defined in [31] to this 2-bitstring probability space.

We say the probability space $(B^n \times B^n, 2^{B^n\times B^n}, R_{n^2})$ is *independent* if for all $1 \le k \le n$ and $x_1,\ldots,x_k,\ y_1,\ldots,y_k \in B$ we have

$$\begin{aligned} R_{n^2}(x_1\ldots x_k B^{n-k} \times y_1\ldots y_k B^{n-k}) =& R_{n^2}(x_1\ldots x_{k-1}B^{n-k+1} \times y_1\ldots y_{k-1}B^{n-k+1}) \\ &\times R_{n^2}(B^{k-1}x_kB^{n-k} \times B^{k-1}y_kB^{n-k}) \end{aligned}$$

For all $x,y \in B^{|x|}$ and $0 \le k+|x| \le n$ we have

$$P_{n^2}(B^{n-k}xB^{n-k-|x|} \times B^{n-k}yB^{n-k-|x|}) = P_{|x|^2}((x,y)).$$

Indeed, using the additivity of the Hamming distance and the $\#_x$ functions, e.g. $d(x_1\ldots x_k, y_1\ldots y_k) = d(x_1\ldots x_{k-1}, y_1\ldots y_{k-1}) + d(x_k, y_k)$, we have:

$$\begin{aligned} P_{n^2}(B^{n-k}xB^{n-k-|x|} \times B^{n-k}yB^{n-k-|x|}) &= \sum_{a_1,a_2\in B^{n-k}}\sum_{b_1,b_2\in B^{n-k-|x|}} P_{n^2}((a_1xb_1, a \\ &= P_{|x|^2}((x,y))\sum_{a_1,a_2\in B^{n-k}}\sum_{b_1,b_2\in B^{n-k-|x|}} P_{(\\ &= P_{|x|^2}((x,y))P_{(n-|x|)^2}(B^{n-|x|}\times B^{n-|x|}) \\ &= P_{|x|^2}((x,y)). \end{aligned}$$

As a direct consequence we deduce that the probability space P_{n^2} defined above is independent.

We now consider the situation where the two output bitstrings x and y are XOR'd against each other (effectively using one as a one-time pad for the other) to produce a single bitstring, and we investigate the distribution of the resulting bitstring. Rather than only considering the effect of XORing paired (and potentially correlated) bits, we also consider XORing outcomes shifted by $j > 0$ bits..

For $j \ge 0$ and $x,y \in B^{n+j}$ define the offset-XOR fucntion $X_j : B^{n+j}\times B^{n+j} \to B^n$ as $X_j(x,y) = z$ where $z_i = x_i \oplus y_{i+j}$ for $i = 1,\ldots,n$. For $z \in B^n$ the set of pairs (x,y) which produce z when XOR'd with offset j is

$$A_j(z) = \{(x,y) \mid x,y \in B^{n+j}, X_j(x,y) = z\} = \{(ua, b(u \texttt{ XOR } z) \mid u \in B^n, a, b \in$$

The probability space of the output produced by the quantum random number generator is $(B^n, 2^{B^n}, Q_{n,j})$, where $Q_{n,j} : 2^{B^n} \to [0,1]$ is defined for all $X \subseteq B^n$ as:

$$Q_{n,j}(X) = \sum_{z\in X} P_{(n+j)^2}(A_j(z)). \tag{3}$$

We note that $|A_j(z)| = 2^{n+2j}$ and check this is a valid probability space. Indeed, $Q_{n,j}(\emptyset) = 0$, is trivially true,

$$Q_{n,j}(B^n) = \sum_{z\in B^n} P_{(n+j)^2}(A_j(z)) = P_{(n+j)^2}\left(\bigcup_z A_j(z)\right) = P_{(n+j)^2}\left(B^{n+j}\times B^{n+}\right.$$

bcause all $A_j(z)$ are disjoint and thus

$$|\bigcup_z A_j(z)| = 2^n 2^{n+2j} = (2^{n+j})^2, \text{ so } \bigcup_z A_j(z) = B^{n+j}\times B^{n+j},$$

and for disjoint $X, Y \subseteq B^n$ we have $Q_{n,j}(X\cup Y) = Q_{n,j}(X) + Q_{n,j}(Y)$.

We now explore the form of the XOR'd distribution $Q_{n,j}$ for $j = 0$ and $j > 0$.

Let $z \in B^n$ and $j \ge 0$. By $z[m,k]$ we denote the substring $z_m\ldots z_k$ for $1 \le m \le k \le n$. We have

$$\begin{aligned} Q_{n,j}(z) =& P_{(n+j)^2}(A_j(z))) \\ =& \sum_{a,b\in 2^j}\sum_{u\in 2^n} P_{(n+j)^2}((ua, b(u \texttt{ XOR } z)) \\ =& \sum_{u\in 2^n} P_{(n-j)^2}((u[j+1,n], (u \texttt{ XOR } z)[1,n-j])) \\ & \cdot \sum_{a\in 2^j} P_{j^2}((a, (u \texttt{ XOR } z)[n-j+1,n]))\sum_{b\in 2^j} P_{j^2}((u[1,j], b)). \end{aligned}$$

For $j=0$, we note that $d(u,u\,\texttt{XOR}\,z)=\#_1(z)$, and thus we have:

$$\begin{aligned}Q_{n,0}(z) &= \sum_{u\in 2^n} P_{n^2}\left((u,(u\,\texttt{XOR}\,z))\right)\\ &= \frac{1}{Z_n}(\sin^2\theta)^{\#_1(z)}(\cos^2\theta)^{\#_0(z)}\sum_{u\in B^n}(e_0^{\oplus})^{\#_0(u)}(e_1^{\oplus})^{\#_1(u)}(e_0^{\otimes})^{\#_0(u\,\texttt{XOR}\,z)}(e_1^{\otimes})^{\#_1(u\,\texttt{XOR}\,z)}\\ &= \frac{1}{Z_n}\left(\sin^2\theta(e_0^{\oplus}e_1^{\otimes}+e_1^{\oplus}e_0^{\otimes})\right)^{\#_1(z)}\left(\cos^2\theta(e_0^{\oplus}e_0^{\otimes}+e_1^{\oplus}e_1^{\otimes})\right)^{\#_0(z)}.\end{aligned}$$

We recognize this as a constantly biased source where

$$p_0=\cos^2\theta(e_0^{\oplus}e_0^{\otimes}+e_1^{\oplus}e_1^{\otimes})/Z_1,\; p_1=\sin^2\theta(e_0^{\oplus}e_1^{\otimes}+e_1^{\oplus}e_0^{\otimes})/Z_1.$$

It is interesting to compare the form of $Q_{n,0}$ to the distribution of the constantly biased source Eq. (2) by discarding one output string—the former is more sensitive to misalignment, the latter to differences in detection efficiencies. In the case of perfect/equal detector efficiencies (but non-perfect misalignment), discarding one string produces uniformly distributed bitstrings, whereas XORing does not.

We now look at the case where $j>0$. For the ideal situation of $\theta=\pi/4$ we have the same result as for the $j=0$ case, while if we have equal detector efficiencies then we get the uniform distribution. We show this as follows (note that $Z_{n+j}=2^{n+j}$ in this case):

$$\begin{aligned}Q_{n,j}(z) =& 2^{-n-j}\sum_{u_n\in B}\cdots\sum_{u_{n-j}\in B}(\sin^2\theta)^{u_n\oplus z_{n-j}\oplus u_{n-j}}(\cos^2\theta)^{1-u_n\oplus z_{n-j}\oplus u_{n-j}}\cdots\\ &\times\sum_{u_1\in B}(\sin^2\theta)^{u_j+1\oplus z_1\oplus u_1}(\cos^2\theta)^{1-u_j+1\oplus z_1\oplus u_1}\\ =& 2^{-n-j}\sum_{u_n\in B}\cdots\sum_{u_{n-j}\in B}(\sin^2\theta+\cos^2\theta)\cdot\sum_{u_1\in B}(\sin^2\theta+\cos^2\theta)\\ =& 2^{-n-j}\sum_{u_{n-j+1}\ldots u_n\in B^j}1\\ =& 2^{-n}.\end{aligned}$$

However, in the more general case of non-equal detector efficiencies, the distribution is no longer independent, although in general is much closer to the uniform distribution than the $j=0$ case. (Recall that independence is a sufficient but not necessary condition for uniform distribution [31].) It is indeed this "closeness"—the total variation distance given by $\Delta(U_n,Q_{n,j})=\frac{1}{2}\sum_{x\in B^n}|2^{-n}-Q_{n,j}(x)|$—which is the important quantity (U_n is the uniform distribution on n-bit strings). However, since $Q_{n,j}$ for $j>0$ is not independent, von Neumann normalization cannot be applied to guarantee the uniform distribution; indeed the dependence is not even bounded to a fixed number of preceding bits.

The problem of determining how best to obtain the maximum amount of information from the quantum random number generator is largely a problem of randomness extractors [32], and is a trade off between the number of uniformly distributed bits obtained and the processing cost—a suitable extractor needs to operate in real-time for most purposes. As we have seen, the fact that two (potentially correlated) bitstrings are obtained allows more efficient operation than a quantum random number generator using single-photons. We have shown how the proposed quantum random number generator can be operationalized in more than one way: either by using shifted XORing of bits to sample from a distribution which is close to (equal to in the ideal limit) the uniform distribution and efficient and robust to various errors, or by utilizing both produced bitstrings to allow a more efficient normalization procedure giving (in absence of the aforementioned temporal effects) the uniform distribution. Many more operationalizations are undoubtedly possible.

[1] The brackets indicate an intuitive, nonformal and heuristic understanding of the term randomness, in contrast to the formalized notions based on algorithmic information theory and statistics.

[2] Erwin Schrödinger, *The Interpretation of Quantum Mechanics. Dublin Seminars (1949-1955) and Other Unpublished Assays* (Ox Bow Press, Woodbridge, Connecticut, 1995).

[3] Cristian S. Calude, Michael J. Dinneen, Monica Dumitrescu, and Karl Svozil, "Experimental evidence of quantum randomness incomputability," Phys. Rev. A **82**, 022102 (2010).

[4] Actually, in a formally precise sense, any finite prefix sequence that is subjectively considered "random" or not, is consistent with formal randomness in a transfinite regime.

[5] Erwin Schrödinger, "Die gegenwärtige Situation in der Quantenmechanik," Naturwissenschaften **23**, 807–812, 823–828, 844–849 (1935), English translation in Ref. [33] and in Ref. [34, pp. 152-167].

[6] Erwin Schrödinger, "Discussion of probability relations between separated systems," Mathematical Proceedings of the Cambridge Philosophical Society **31**, 555–563 (1935).

[7] Erwin Schrödinger, "Probability relations between separated systems," Mathematical Proceedings of the Cambridge Philosophical Society **32**, 446–452 (1936).

[8] Anton Zeilinger, "A foundational principle for quantum me-

chanics," Foundations of Physics **29**, 631–643 (1999).

[9] Albert Einstein, Boris Podolsky, and Nathan Rosen, "Can quantum-mechanical description of physical reality be considered complete?" Physical Review **47**, 777–780 (1935).

[10] Simon Kochen and Ernst 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. [35, pp. 235–263].

[11] Cristian S. Calude and Karl Svozil, "Quantum randomness and value indefiniteness," Advanced Science Letters **1**, 165–168 (2008), arXiv:quant-ph/0611029.

[12] Karl Svozil, "The quantum coin toss—testing microphysical undecidability," Physics Letters A **143**, 433–437 (1990).

[13] 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).

[14] Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger, "Violation of Bell's inequality under strict Einstein locality conditions," Physical Review Letters **81**, 5039–5043 (1998).

[15] Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger, "A fast and compact quantum random number generator," Review of Scientific Instruments **71**, 1675–1680 (2000), quant-ph/9912118.

[16] André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden, "Optical quantum random number generator," Journal of Modern Optics **47**, 595–598 (2000).

[17] P. X. Wang, G. L. Long, and Y. S. Li, "Scheme for a quantum random number generator," Journal of Applied Physics **100**, 056107 (2006).

[18] Ma Hai-Qiang, Wang Su-Mei, Zhang Da, Chang Jun-Tao, Ji Ling-Ling, Hou Yan-Xue, and Wu Ling-An, "A random number generator based on quantum entangled photon pairs," Chinese Physics Letters **21**, 1961–1964 (2004).

[19] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, "Secure self-calibrating quantum random-bit generator," Physical Review A **75**, 032334 (2007).

[20] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).

[21] Artur K. Ekert, "Quantum cryptography based on Bell's theorem," Physical Review Letters **67**, 661–663 (1991).

[22] Helle Bechmann-Pasquinucci and Asher Peres, "Quantum cryptography with 3-state systems," Physical Review Letters **85**, 3313–3316 (2000).

[23] Karl Svozil, "Three criteria for quantum random-number generators based on beam splitters," Physical Review A **79**, 054306 (2009), arXiv:quant-ph/0903.2744.

[24] Karl Svozil, "Quantum value indefiniteness," Natural Computing **online first**, 1–12 (2010), arXiv:1001.1436.

[25] J.-W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, "Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement," Nature **403**, 515–519 (2000).

[26] Yun-Feng Huang, Chuan-Feng Li, Yong-Sheng Zhang, Jian-Wei Pan, and Guang-Can Guo, "Experimental test of the Kochen-Specker theorem with single photons," Physical Review Letters **90**, 250401 (2003), quant-ph/0209038.

[27] Adan Cabello, "Experimentally testable state-independent quantum contextuality," Physical Review Letters **101**, 210401 (2008).

[28] Alastair A. Abbott, Cristian S. Calude, and Karl Svozil, "Incomputability of quantum randomness," in preparation (2010).

[29] B^n is the set of bitstrings x of length $|x| = n$; 2^X is the set of all subsets of the set X.

[30] Patrick Billingsley, *Probability and Measure* (John Wiley & Sons, New York, Toronto, London, 1979).

[31] Alastair A. Abbott and Cristian S. Calude, *von Neumann Normalisation of a Quantum Random Number Generator*, Report CDMTCS-392 (Centre for Discrete Mathematics and Theoretical Computer Science, University of Auckland, Auckland, New Zealand, 2010).

[32] Ariel Gabizon, *Deterministic Extraction from Weak Random Sources* (Springer, Berlin Heidelberg, 2010).

[33] 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. [34, pp. 152-167].

[34] John Archibald Wheeler and Wojciech Hubert Zurek, *Quantum Theory and Measurement* (Princeton University Press, Princeton, NJ, 1983).

[35] Ernst Specker, *Selecta* (Birkhäuser Verlag, Basel, 1990).