# Quantum randomness and value indefiniteness

Cristian S. Calude*†

*Department of Computer Science, The University of Auckland,*

*Private Bag 92019, Auckland, New Zealand*

Karl Svozil‡

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

*Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria*

## Abstract

As computability implies value definiteness, certain sequences of quantum outcomes cannot be computable.

Keywords: Quantum information, quantum randomness, time series analysis, noise

* Work done at the University of Technology Vienna: the support of the Institute for Theoretical Physics is gratefully acknowledged.

†Electronic address: cristian@cs.auckland.ac.nz; URL: http://www.cs.auckland.ac.nz/~cristian/

‡Electronic address: svozil@tuwien.ac.at; URL: http://tph.tuwien.ac.at/~svozil

## I. CONCEPTUALISATION

It certainly would be fascinating to pinpoint the time of the emergence of the notion that certain quantum processes, such as the decay of an excited quantum state, occurs principally and irreducibly at random; and how long it took to become the dominant way of thinking about them after almost two centuries of quasi-rationalistic dominance. Bohr's and Heisenberg's influence has been highly recognised and has prevailed, even against the strong rationalistic and philosophic objections raised by, for instance, by Einstein and Schrödinger [1, 2]. Of course, one of the strongest reasons for this growing acceptance of quantum randomness has been the factual inability to go "beyond" the quantum in any manner which would encourage new phenomenology and might result in any hope for a progressive quasi-classical research program [3].

Here we intend to discuss quantum randomness and its connection with quantum value indefiniteness. Bell [4–7], Kochen and Specker (KS) [8], as well as Greenberger, Horne and Zeilinger (GHZ) [9–11] contributed to the evidence that the mere concept of coexistence of certain elements of physical reality [12] results in a complete contradiction. In this view, speculations about the "reasons" for certain outcomes of experiments are necessarily doomed; just because of the simple fact that any such rational reason is provably (by contradiction) impossible.

An attempt is made here to clearly spell out the issues and problems involved in considering randomness, both with regard to the occurrence of single events, as well as their combination into time series. We wish to state from the beginning that we attempt to have no bias or preference for or against randomness. While to us it seems obvious that any claim of non-randomness has to be confronted with the factual inability to produce any satisfactory theory that goes beyond the quantum, especially in view of the known no-go theorems by Bell, KS and GHZ and others referred to above, it is also advisable to keep all options open and carefully study the types of randomness involved, and their possible "origins," if any.

Usually, the random outcome of certain quantum physical events seems to be axiomatically postulated from the onset; an assumption which can be also based on elementary principles [13, 14]. Here we argue that actually we can go further and infer some properties of quantum randomness — including the absence of effective global correlations — from the

impossibility of value definiteness of certain quantum mechanical observables.

### A. Difficulties

Consider, as two extreme cases, the binary expansion $\pi_1\pi_2\pi_3\ldots\pi_i\pi_{i+1}\ldots$ of pi, an ideal circle's ratio of the circumference to its diameter, starting from, say, the 571113th billion prime number place onwards, and compare it to a sequence generated by quantum coin tosses $x_1x_2x_3\ldots x_ix_{i+1}\ldots$ [15–17]. How could anyone possibly see a difference with respect to their (non-)stochasticity? For all practical purposes, the sequences will appear structurally identically from a stochastic point of view, and heuristically random. For example, both are unknown to be Borel normal; i.e., all finite sub-sequences $y_1y_2y_3\ldots y_N$ might be contained in them with the expected frequencies. Indeed, it is not unreasonable to speculate that the pi sequence might be immune to all statistical and algorithmic tests of randomness but one: a test against the assumption that it is the binary expansion of pi, starting from the 571113th billion prime number place onwards.

Another obstacle for the physical conceptualisation of quantum randomness and its operationalisation in terms of physical entities originates in the formalism upon which such endeavours have to be based. The formal incompleteness and independence discovered by Gödel, Tarski, Turing, Chaitin and others essentially renders algorithmic proofs of randomness hopeless. We shall discuss these issues below, but we just note that, as an example, verification of any "law" describable by $k$ symbols requires times exceeding any computable function of $k$ [such as the Ackermann function $A(k)$] and could in general take also that long to be falsified. Thus, the proof of any absence of lawful behaviour seems provable impossible.

Randomness is an asymptotic property, that is, it is unaffected by finite variations. This makes testing randomness extremely difficult: one has to find finite tests capable of distinguishing an infinite behaviour.

### B. Scenarios

Quantum randomness appears to occur in two different scenarios: (i) the complete impossibility to predict or explain the occurrence of certain *single* events and measurement outcomes from any kind of operational causal connection. The hidden "parameter models"

for the quantum phenomena which have been proposed so far do not provide more insight for the predictions of intrinsic observers embedded in the system; and (ii) the concatenation of such single quantum random events forms sequences of random bits which can be expected to be equivalent stochastically to white noise. White noise carries the least correlations, as the occurrence of a particular bit value in a binary expansion does not depend on previous or future bits of that expansion [18].

These different ways to encounter randomness — single random events and a concatenation thereof — should be perceived very differently: in the single event case, the outcome occurs in the highly complex environment of the quantum and its measurement apparatus, which is thereby "folded" into a single bit. Repetition of the experiment does not increase the complexity of the combined system of the quantum–measurement apparatus, whose repetitive properties and behaviours are "unfolded" in repeated experiments. Hence, possible biases against statistical tests may be revealed easier by considering sequences of single random outcomes. In this note we shall thus concentrate on this second.

### C. Axioms for quantum randomness and degrees of randomness

In what follows, we will assume the standard two "axioms" for quantum randomness [19]:

- The single outcome from which quantum random sequences are formed, occurs unbiased; i.e., for the $i$th outcome, there is a 50:50 probability for either 0 or 1:

$$\text{Prob}(x_i = 0) = \text{Prob}(x_i = 1) = \tfrac{1}{2}. \tag{1}$$

- There is a total independence of previous history, such that no correlation exists between $x_i$ and previous or future outcomes. This means that the system carries no memories of previous or expectations of future events. All outcomes are temporally "isolated" and free from control, influence and determination. They are both unbiased and self-contained.

Assume that we have a quantum experiment (using light, for example: a photon generated by a source beamed to a semitransparent mirror is *ideally* reflected or transmitted with 50 per cent chance) which at each stage produces a quantum random bit, and we assume that

this experiment is run for ever generating an infinite binary sequence:

$$X = x_1 x_2 x_3 \cdots x_i \cdots \tag{2}$$

In this scenario, the first axiom shows that the limiting frequency of 0 and 1 in the sequence $X$ is $1/2$. Locally, we might record significant deviations, i.e., $X$ may well start with a thousand of 1's, but in the limit these discrepancies disappear.

The "lack of correlations" postulated above is more difficult to understand and may easily lead to misunderstandings, hence errors. First, *finite correlations* will always exist, because of the asymptotic nature of "randomness". Secondly, even *infinite correlations* cannot be eliminated because they have been proven to exist in *every infinite sequence*; for example Ramsey-type correlations, see [20]. So, what type of correlations should be prohibited? There are many possible choices, but the ones which come naturally to mind are "effectively computable defined correlations." In other terms, correlations — finite or infinite — which can be detected in an effective/algorithmic way, should be excluded.

Once the nature of the two axioms of randomness has been clarified, we can ask ourselves whether we need both axioms, that is, whether the axioms are *independent*. The answer is *affirmative* and here is the proof. An example of a binary sequence which satisfies the first axiom, but not the second axiom is Champernowne's sequence $0100011011000001010011 \cdots 1110000 \cdots$, which is just the concatenation of all binary strings in quasi-lexicographical order. In this sequence 0 and 1 have limiting frequency $1/2$ (even, more, each string of length $n$ has limiting frequency exactly $1/2^n$), but, of course, this sequence is computable, so it contains infinitely many finite and infinite correlations.

It is possible to transform a sequence $Z = z_1 z_2 \cdots$ with no correlations and limiting frequency of 0's (and 1's) exactly $1/2$ into a sequence which has no infinite correlations, but the limiting frequency of 0's is $2/3$ and the limiting frequency of 1's is $1/3$: replace in $Z$ every 0 by 001, and every 1 by 100. This new sequence will have "weak local correlations" — for example 0010 has to be followed by 01 — but those correlations are not global.

We stress the fact that we are interested in "theoretical" sequences (2) produced by an ideal quantum experiment generating randomness, not the specific results of a particular quantum device like *Quantis*, [21]. Real devices are prone to real-world imperfections, even watered-down by various unbiasing methods, see [17]; however, our results apply in the limit to sequences generated by devices like *Quantis* (see [17, 22]).

What is the degree of "randomness" of the resulting white noise sequence? Theoretically there are a few possibilities, ranging from "total randomness" expressed mathematically by saying that the sequence is algorithmically incompressible or algorithmically random,[20] to weaker and weaker possibilities: Turing-uncomputable of various degrees, but not algorithmically incompressible, Turing-computable, easy Turing-computable. Which of these possibilities actually does occur?

## II. MAIN RESULTS

### A. Quantum value indefiniteness

In classical physics, omniscience manifests itself in the implicit assumption that it is possible to know all physical properties, or to put it in the context of the Einstein, Podolsky and Rosen argument [12], all "elements of physical reality" are definite. Classical realism assumes that these definite physical properties exist without being experienced by any finite mind [23], that it would not matter whether or not a particular physical observable is measured or not; and that the outcome of any such measurement is independent of whatever is measured alongside with it; that is, of its context. To state it pointedly: all classical physical observables exist simultaneously and independent of observation.

Complementarity expresses the impossibility to measure two observables, such as the spin states of two spin-$\frac{1}{2}$ particles along orthogonal directions, with arbitrary precision. But, as equivalent [24] generalised urn [25] or automaton models [26] demonstrate, complementarity does not necessarily imply value indefiniteness. There still could exist enough two-valued states on the associated propositional structures to allow a faithful embedding into a Boolean algebra associated with classical physical systems. Formally, value indefiniteness manifests itself in the "scarcity" or non-existence of two-valued states –interpretable as classical truth assignments – on all or even merely a finite set of physical observables. This is known as the Kochen-Specker theorem [8] (for related results, see Refs. [27–31]). Very similar conclusions can be drawn from the impossibility to enumerate tables of results associated with Bell-type experiments in a consistent way: no such tables could possibly reproduce the non-classical quantum correlations [32–34].

Confronted with the impossibility to consistently assign globally defined observables, one

may assume, in an attempt to maintain realism, that the outcome of a particular experiment depends on the other observables which are co-measured simultaneously (Bell [4], Sec. 5). This assumption is called "context dependence."

Alternatively, one may depart from classical omniscience and assume that an elementary two-state system can carry at least a single bit, and nothing more. The context enters in the form of the maximal operator, such that all other co-measurable operators are functions thereof. If a particle can be prepared only to be in a single context, then the question quite naturally arises why the measurement of a different context not matching the preparation context yields any outcome at all. Pointedly stated, it is amazing that *for non-matching contexts there is an outcome rather than none.* We note that only under these circumstances, quantum randomness manifests itself, because if the preparation and the measurement contexts match, the measurement just renders the definite outcome associated with the state in which the particle was prepared. In this non-contextual view, quantum value indefiniteness expresses the fact that no deterministic, (pre-) defined non-contextual element of physical reality could consistently exist for observables in contexts not matching the preparation context. This is true also if we assume some form of "context translation" which may introduce stochasticity through some mechanism of interaction with the measurement device.

### B. From value indefiniteness to Turing-uncomputability

Thus, we conclude, *no non-contextual, deterministic computation could exist which yields such a measurement outcome.* If one insists on some form of agent producing the outcome, then this agent must perform like an erratic gambler rather than a faithful executor of a deterministic algorithm.

Restated differently, suppose a quantum sequence hitherto considered would be computable. In this case, the computations involved would produce a definite number associated with a definite outcome, which in turn could be associated with a definite element of physical reality. Yet we know that for Hilbert spaces of dimension greater than two, the assumption of value definiteness of all possible observables results in a complete contradiction. Hence, one is forced to conclude that *the assumption of computability has to be given up, and hence the sequence $X$ in (2) is Turing-uncomputable.*

Because the class of computable sequences is countable, with probability one (even, con-

structively, with probability one, see [20]) every sequence is Turing-uncomputable. Our result stated above is much stronger: *no sequence $X$ in (2) is Turing-computable.* In particular, it says that any sequence $X$ cannot contain only 0's, it cannot represent in binary the digits of the binary expansion of pi or the Champernowne sequence. More, no sequence $X$ can coincide with a pseudo-random sequence (i.e., sequence obtain via Turing machine program), a fact alluded to almost 50 years ago by John von Neumann: "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin".

### C. White noise and algorithmic incompressibility

Uncomputability is a strong property, but it does not necessarily imply algorithmically incompressibility. Is a sequence $X$ more similar to the typical Turing-uncomputable sequence given by the classification of Turing programs in halting or non-halting,

$$H = h_1 h_2 h_3 \cdots h_i \cdots, \tag{3}$$

or to the sequence of bits of a Chaitin Omega number, the halting probability:

$$\Omega = \omega_1 \omega_2 \omega_3 \cdots \omega_i \cdots? \tag{4}$$

The sequence $H$ is defined by assigning to $h_i$ the value 1 if the $i$th Turing program (in some systematic enumeration) halts, and the value 0 in the opposite case.

The sequence $\Omega$ is obtained by working with self-delimiting Turing machines (i.e. machines with prefix-free domains) by the formula:

$$\Omega = \sum_{p \text{ halts}} 2^{-|p|},$$

where $|p|$ denotes the length (in bits) of the program $p$ (see more in [20]).

Both $H$ and $\Omega$ are Turing-uncomputable. The sequence $H$ is Turing-uncomputable, but it is also not algorithmic incompressible. A reason is the fact that we can effectively compute infinitely many exact values of $H$ by explicitly constructing infinitely many halting (or, non-halting) programs. The sequence $\Omega$ is algorithmic incompressible. Both $H$ and $\Omega$ can solve the famous Halting Problem: we need the first $2^n$ bits of $H$ to solve the Halting Problem for programs $p$ of length $|p| \leq n$, but we need no more than the first $n$ bits of $\Omega$ to solve the

same problem. The prefixes of $\Omega$ encode the same amount of information as the prefixes of $H$, but in an exponentially more compressed way.

It is not difficult to see that the argument presented below to show that $X$ is Turing-uncomputable can be adapted to prove that *every infinite sub-sequence of $X$ is Turing-uncomputable.* More formally, *there is no partially computable function $\varphi$ defined on an infinite set of positive integers such that if $\varphi(n)$ is defined, then $\varphi(n) = x_n$.* This property is called *bi-immunity* in the theory of computability, see Odiffredi [35].

This property is shared by $\Omega$, but not by $H$.

### D. Some consequences

We discuss some simple consequences of the above result.

First, no Turing machine can enumerate/compute any sub-sequence of $X$. This means that every given Turing machine can compute only finitely many exact bits of $X$ in the same way that every given Turing machine can compute only finitely many exact bits of $\Omega$ (in contrast with $H$). Similarly, any formal system (ZFC, for example) will be able to "prove" only finitely many exact values of the sequence $X$.

Secondly, the sequence $X$ is *not predictable.* The most clear intuition people have about randomness is unpredictability: the bits of a "random" sequence should be such that one cannot predict the next bit even if one knows all preceding bits. The simplest way to model this phenomenon (see other models in [36]) is to consider predictions of the $(n+1)$th element of the sequence when one knows the first $n$ elements. The corresponding model is to accept as *predictor* a partial computable function $Pred$ defined on a subset of the prefixes of $X$ with 0-1 values. If $Pred(w) = z$ and $z = x_{|w|+1}$ we say that the bit $z$ was predicted from $w$. Does there exist a predictor $Pred$ predicting infinitely many bits of $X$? The answer is clearly negative: from $Pred$ we can construct a partially computable function $\varphi$ capable of enumerating infinitely many values of $X$ just by enumerating the domain of $Pred$ and each time we get $Pred(w) = z$ and $z = x_{|w|+1}$, then we put $\varphi(|w|) = z$. This leads to a contradiction.

Thirdly, a more general result can be proved: *there are no effective global (infinite) correlations between the bits of $X$.* One way to formalise this idea is to consider all possible properties between the prefixes of $X$ that can be determined in an effective way. We can prove

the following result: *Every infinite relation of the form* $G = \{(u, v) \mid uv$ *is a prefix of* $X\}$ *is not computably enumerable.* Indeed, from $G$ we can construct the partial function $\varphi$ as follows: to the pair $(u, v) \in G, v = v_1 v_2 \cdots v_m$ we associate the following values of $\varphi$: $\varphi(|u| + i - 1) = v_i, i = 1, \ldots, m$. The function $\varphi$ is correctly defined because of the condition specified in the definition of $G$; it shows that one can effectively enumerate infinitely many bits of $X$, a contradiction.

## III. SUMMARY AND DISCUSSION

We have argued that, because of the value indefiniteness encountered in quantum mechanics, there cannot exist deterministic computations "yielding" infinitely many individual quantum random bits. We have further exploited value indefiniteness formally by stating the consequences in terms of Turing-uncomputability for sequences of such quantum random bits. No effectively computable global correlations can exist between the bits of a quantum random sequence.

We have also examined, in a theoretical manner, the role of the second axiom of quantum randomness. The first axiom, stochasticity, seems more difficult to be studied from a purely theoretical point of view — of course, it will be extremely interesting to have results in this direction — but can be experimentally approached (for example, with the help of statistically significant samples produced by *Quantis*).

Finally, we note that the result presented in this note says nothing about the possibility of extracting quantum bits from the quantum source of randomness, which, one might hope, could enhance the power of "real" computation. Some impossibility results in this direction were proved in [37].

**Acknowledgement**

We thank Ludwig Staiger for illuminating discussions on bi-immunity and stochasticity.

---

[1] M. Jammer, *The Conceptual Development of Quantum Mechanics* (McGraw-Hill Book Company, New York, 1966).

[2] M. Jammer, *The Philosophy of Quantum Mechanics* (John Wiley & Sons, New York, 1974).

[3] I. Lakatos, *Philosophical Papers. 1. The Methodology of Scientific Research Programmes* (Cambridge University Press, Cambridge, 1978).

[4] J. S. Bell, "On the Problem of hidden variables in quantum mechanics," Reviews of Modern Physics **38**, 447–452 (1966). Reprinted in [6, pp. 1-13], URL `http://dx.doi.org/10.1103/RevModPhys.38.447`.

[5] J. S. Bell, "On the Einstein Podolsky Rosen paradox," Physics **1**, 195–200 (1964). Reprinted in [38, pp. 403-408] and in [6, pp. 14-21].

[6] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, 1987).

[7] I. Pitowsky, "From George Boole to John Bell: The origin of Bell's inequality," in *Bell's Theorem, Quantum Theory and the Conceptions of the Universe*, M. Kafatos, ed., pp. 37–49 (Kluwer, Dordrecht, 1989).

[8] S. Kochen and E. P. Specker, "The Problem of Hidden Variables in Quantum Mechanics," Journal of Mathematics and Mechanics **17**(1), 59–87 (1967). Reprinted in [39, pp. 235–263].

[9] 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., pp. 73–76 (Kluwer Academic Publishers, Dordrecht, 1989).

[10] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, "Bell's theorem without inequalities," American Journal of Physics **58**, 1131–1143 (1990).

[11] 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).

[12] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" Physical Review **47**, 777–780 (1935). URL `http://dx.doi.org/10.1103/PhysRev.47.777`.

[13] A. Zeilinger, "A Foundational Principle for Quantum Mechanics," Foundations of Physics **29**(4), 631–643 (1999). URL `http://dx.doi.org/10.1023/A:1018820410908`.

[14] Č. Brukner and A. Zeilinger, "Information and fundamental elements of the structure of quantum theory," in *Time, Quantum and Information*, L. Castell and O. Ischebek, eds., pp. 323–355 (Springer, Berlin, 2003). quant-ph/0212084.

[15] K. Svozil, "The quantum coin toss—Testing microphysical undecidability," Physics Letters A **143**, 433–437 (1990). URL http://dx.doi.org/10.1016/0375-9601(90)90408-G.

[16] 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). quant-ph/9912118, URL http://dx.doi.org/10.1063/1.1150518.

[17] C. S. Calude, "Algorithmic randomness, quantum physics, and incompleteness," in *Proceedings of the Conference "Machines, Computations and Universality" (MCU'2004)*, M. Margenstern, ed., pp. 1–17 (Lectures Notes in Comput. Sci. 3354, Springer, Berlin, 2005).

[18] M. Gardner, "White and brown music, fractal curves and one-over-$f$ fluctuations," Scientific American **238**, 16–32 (1978). See also URL http://www.seriouscomposer.com/TDML/tdml.htm.

[19] J. M. Jauch, *Foundations of Quantum Mechanics* (Addison-Wesley, Reading, MA., 1968).

[20] C. Calude, *Information and Randomness—An Algorithmic Perspective*, 2nd ed. (Springer, Berlin, 2002).

[21] id Quantique, "Quantis - Quantum Random Number Generators," (2004). URL http://www.idquantique.com.

[22] M. J. Dinneen, C. S. Calude, "Is quantum randomness algorithmic random? A preliminary attack," in *Proceedings of the 1st International Conference on Algebraic Informatics*, G. R. S. Bozapalidis, A. Kalampakas, ed., pp. 195–196 (Aristotle University of Thessaloniki, 2005).

[23] W. T. Stace, "The Refutation of Realism," in *Readings in philosophical analysis*, H. Feigl and W. Sellars, eds. (Appleton–Century–Crofts, New York, 1949). Previously published in *Mind* **53**, 1934.

[24] K. Svozil, "Logical equivalence between generalized urn models and finite automata," International Journal of Theoretical Physics **44**, 745–754 (2005). quant-ph/0209136, URL http://dx.doi.org/10.1007/s10773-005-7052-0.

[25] R. Wright, "Generalized urn models," Foundations of Physics **20**, 881–903 (1990).

[26] K. Svozil, *Quantum Logic* (Springer, Singapore, 1998).

[27] N. Zierler and M. Schlessinger, "Boolean embeddings of orthomodular sets and quantum logic," Duke Mathematical Journal **32**, 251–262 (1965).

[28] V. Alda, "On 0-1 measures for projectors I," Aplik. mate. **25**, 373–374 (1980).

[29] V. Alda, "On 0-1 measures for projectors II," Aplik. mate. **26**, 57–58 (1981).

[30] F. Kamber, "Die Struktur des Aussagenkalküls in einer physikalischen Theorie," Nachr. Akad. Wiss. Göttingen **10**, 103–124 (1964).

[31] F. Kamber, "Zweiwertige Wahrscheinlichkeitsfunktionen auf orthokomplementären Verbänden," Mathematische Annalen **158**, 158–196 (1965).

[32] A. Peres, "Unperformed experiments have no results," American Journal of Physics **46**, 745–747 (1978). URL `http://dx.doi.org/10.1119/1.11393`.

[33] G. Krenn, "The Probabilistic Origin of Bell's Inequality," in *Proceedings of the Third International Workshop on Squeezed States and Uncertainty Relations, Maryland, August 10-13, 1993, NASA Conference publication Nr. 3270*, D. Han, Y. S. Kim, N. H. Rubin, Y. Shih, and W. W. Zachary, eds., pp. 603–608 (NASA, Greenbelt, Maryland 20771, 1993).

[34] G. Krenn and K. Svozil, "Stronger-than-quantum correlations," Foundations of Physics **28**(6), 971–984 (1998). URL `http://dx.doi.org/10.1023/A:1018821314465`.

[35] P. Odifreddi, *Classical Recursion Theory, Vol. 2* (North-Holland, Amsterdam, 1999).

[36] D. H. R. Downey, *Algorithmic Randomness and Complexity* (Springer, Berlin, 2007). To appear.

[37] Y. Dodis and R. Renner, "On the impossibility of extracting classical randomness using a quantum computer," in *ICALP 2006, Part II*, M. Bugliese, B. Preneel, V. Sassone, and I. Wegener, eds., pp. 204–215 (LNCS 4052, Springer, Heidelberg, 2006).

[38] J. A. Wheeler and W. H. Zurek, *Quantum Theory and Measurement* (Princeton University Press, Princeton, 1983).

[39] E. Specker, *Selecta* (Birkhäuser Verlag, Basel, 1990).