Quantum and Algorithmic Randomness

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

Abstract

To be written later

PACS numbers: 03.65.Ta,03.65.Ud

Keywords: quantum randomness, value indefiniteness, incomputability, Martin-Löf randomness

[*] c.calude@auckland.ac.nz; http://www.cs.auckland.ac.nz/˜cristian

[†] svozil@tuwien.ac.at; http://tph.tuwien.ac.at/˜svozil

I. PRELIMINARIES

Cryptographic algorithms require a method of generating a secret key from “random” bits. The strength of the system ultimately depends on the strength of the key used, that is, on the difficulty for an eavesdropper to guess or calculate it. Classical keys are vulnerable, but keys formed with quantum random bits have been claimed to be unbreakable because *quantum randomness is true, irreducible (sometimes called perfect) randomness* (see [15]). Indeed, poor quality randomness are, among other issues, at the root of various failures of quantum cryptographic systems (see [5, 11]), motivating a recent systematic evaluation of the failure rate of these systems [14].

Alas, claims of absolute randomness are false for the following reasons. First, *there is no true randomness, irrespective of the method used to produce it*; or, stated differently by Motzkin, a *“complete disorder is an impossibility. Any structure will necessarily contain an orderly substructure”* [13]. The British mathematician and logician Frank P. Ramsey was the first to demonstrate this in his study of *conditions under which order must appear* (see [9, 13]); other proofs have been given in the framework of algorithmic information theory [3].

Second, randomness on finite strings can neither be proved nor disproved. A proof of non-randomness is impossible because, as already pointed out, by Ramsey theory and other findings, any particular “anecdotal” sequence must occur either as a prefix or “within” a provably infinite random sequence. (Actually, any such sequence occurs infinitely often.) Conversely, a proof of determinism cannot be given, because any proof would at least have to involve the *absence* of any law (let alone algorithmic incompressibility [3]), which would require a solution to the *rule inference problem* [**?**] which in turn can be reduced to the *halting problem*, which is provable unprovable.

These facts point to the necessity to understand better the nature and quality of quantum randomness. In [1, 4] we have made some steps in this direction. Although in practice only finitely many bits are necessary for encrypting a given message, to be able to compare the quality of randomness we need to consider infinite sequences of bits. One important criterion is whether such a sequence is Turing computable (i.e. it can be produced by an algorithm) or not. Pseudo-random sequences are obviously Turing computable; they are easily predictable once we know the algorithm generating the sequence, so, not surprisingly, their quality of randomness is low.

The character and quality of quantum random number generators can, in principle, be “certified,” or at least conjectured, in two ways. The first, syntactic, way is to *create phenotypes* of such sequences through "quantum coin tosses" [? ? ?], and then subjecting it to various statistical or algorithmic tests [?]. The second, semantic, way is to make *assumptions about the source*; in particular physical assumptions such as quantum complementarity or quantum value indefiniteness.

Quantum randomness is not Turing computable under the following assumptions. Suppose the standard quantum mechanical Hilbert space formalism without augmentation of ("contextual, non-local") hidden variables or parameters. By this, we shall also exclude *context translation* [?], in which a *means relative* [?] randomness comes about by the many degrees of freedom of the quantum and the measurement apparatus combined, which, "for all practical purposes" [?] *cannot be resolved by the physical means available.*

Then, preparing a quantum in a particular state and measuring some *complementary* "property" thereof (relative to the property constituting the preparation) results in a *creatio ex nihilo* of some measurement outcome. Any sequence of such outcomes can be encoded symbolically and constitutes a string that, according to the quantum *canon*, is not subject to any *principle of sufficient reason*. According to Philipp Frank [?], any such occurrence amounts to a *gap* in the deterministic representation of physical processes – in short a *miracle*.

This *creatio ex nihilo* is corroborated by another property in standard Hilbert space quantum theory (with the assumption of non-contextuality): *value indefiniteness* [?]. Quantum random generators supported by value indefiniteness are based on an experiment in which a value indefinite observable – that is, an observable which cannot have a definite value, either zero or one, before measurement – is measured. This condition is satisfied by a quantum experiment subject to the Kochen-Specker theorem, a classical result proved 46 years ago for a different aim: to show the impossibility of a deterministic hidden variable theory for quantum mechanics [10]. A quantum random number generator designed in terms of generalised beam splitters implements these theoretical ideas [1]. A sequence of bits generated by this quantum random number generator is highly incomputable: no algorithm can compute more than finitely many bits of the sequence. High incomputability is a symptom of randomness, a necessary but rather weak one.

In this paper we show that sequences generated by the quantum random number generator in [1] are Martin-Löf random...

II. NOTATION

As usual we denote the set of complex numbers by $\mathbb{C}$ and use the standard quantum mechanical bra-ket notation; that is, we denote vectors in the Hilbert space $\mathbb{C}^n$ by $|\cdot\rangle$.

Let $\mathbb{N} = \{0,1,2,3,\ldots\}$ be the set of natural numbers and $\mathbb{N}_+$ be the set of positive integers. The cardinal of a set A is denoted by $\#(A)$. For a tuple $a = (a_1,\ldots,a_k)$ we denote the kth projection as $\Pi_k(a) = a_k$. Let $B = \{0,1\}$; by $B^* = \{\lambda,0,1,00,01,10,11,000,\ldots\}$ we denote the set of finite binary strings, where λ denotes the *empty string*. The set of infinite binary sequences, where an infinite binary sequence is infinite to the right but finite to the left, is denoted by B^∞. For any $\mathbf{x} \in B^\infty$ and $n \in \mathbb{N}_+$, we denote the nth bit of $\mathbf{x}$ by x_n and the prefix of length n of $\mathbf{x}$ by $\mathbf{x}\!\upharpoonright_n \in B^*$. Namely, $\mathbf{x}\!\upharpoonright_0 = \lambda$, and $\mathbf{x}\!\upharpoonright_n = x_1 x_2 \ldots x_n$, for every $n \in \mathbb{N}_+$. The mth section of the set $T \subset B^* \times \mathbb{N}_+$ is $T_m = \{u \in B^* \mid (u,m) \in T\}$.

Computability definitions: computable sets, c.e. set, bi-immune sequence = no algorithm can enumerate the correct values of infinitely many bits of the sequence, AIT: Lebesgue measure μ, Martin-Löf test of randomness,

III. RANDOMNESS

The intuition is that a "random" sequence should be "typical", i.e. should not stand out from the crowd (of all sequences) by having any specific properties. A specific property of a sequence is given by an infinite set of correlations between the bits of the sequence. Some, but not all properties, make a sequence special, atypical, hence non random. For example, the sequence

$$\mathbf{a} = 0101000100000001000000000000000 1\cdots$$

is atypical, as all bits sitting on power of 2 positions are 1.

By flipping a coin "to infinity" we get a sequence $\mathbf{x}$ in which we expect to see as many heads (1) as tails (0). Mathematically this can be expressed by saying that $\mathbf{x}$ obeys the *law of large numbers*, that is

$$\lim_{n\to\infty} (x_1 + x_2 + \cdots + x_n)/n = 1/2. \tag{1}$$

The sequence $\mathbf{x}$ may start with any string of 0s and 1s, for example, with a billion of 0s, but eventually the long run of 0s gets compensated and the uniform distribution of 0s and 1s (cf. (1)) settles down.

Is any sequence satisfying the law of large numbers atypical? The answer is negative. The Champernown sequence

$$01000110110000010100111001011101110000\cdots$$

obeys the law of large numbers [6]; clearly, this is not a random sequence because the algorithm allowing to generate/recognise its bits (enumerate all binary strings in increasing length and for strings of equal length, enumerate in lexicographical order) imposes infinitely many correlations. More generally, any computable sequence is atypical too.

Are there infinite sequences with no infinite set of correlations? The answer given by Ramsey theory [9] is **negative**: *complete disorder is impossible.* This fact puts a very strong restriction on any attempt to define randomness. The only possible solution is to *select* a class of meaningful correlations $\mathcal{C}$ and then define a *$\mathcal{C}$–random sequence* to be a sequence which does not have any correlations in $\mathcal{C}$. Obviously, a "meaningful" (good quality) $\mathcal{C}$–random sequence should not be computable; a minimal requirement is bi-immunity. There are many classes of meaningful $\mathcal{C}$–random sequences, see [7]. Arguably the most important form of randomness is Martin-Löf randomness [3, 7, 12].

IV. VALUE INDEFINITE OBSERVABLES

In what follows we only consider pure quantum states. Projection operators—projecting on to the linear subspace spanned by a non-zero vector $|\psi\rangle$—will be denoted by $P_\psi = \frac{|\psi\rangle\langle\psi|}{\langle\psi|\psi\rangle}$.

We fix a positive integer n. Let $\mathcal{O} \subseteq \{P_\psi \mid |\psi\rangle \in \mathbb{C}^n\}$ be a non-empty set of *projection observables* in the Hilbert space $\mathbb{C}^n$ and $\mathcal{C} \subseteq \{\{P_1, P_2, \dots P_n\} \mid P_i \in \mathcal{O} \text{ and } \langle i|j\rangle = 0 \text{ for } i \neq j\}$ a set of measurement contexts over $\mathcal{O}$. A *context* $C \in \mathcal{C}$ is thus a maximal set of compatible (i.e. they can be simultaneous measured) projection observables. Let $v : \{(o,C) \mid o \in \mathcal{O}, C \in \mathcal{C} \text{ and } o \in C\} \overset{o}{\to} B$ be a partial function (i.e., it may be undefined for some values in its domain) called *assignment function*. For some $o, o' \in \mathcal{O}$ and $C, C' \in \mathcal{C}$ we say $v(o,C) = v(o',C')$ if $v(o,C), v(o',C')$ are both defined and have equal values.

Value definiteness corresponds to the classical notion of determinism: an observable is value definite if v assigns it a definite value—i.e. is able to predict in advance, independently of measurement, the value obtained via measurement. Here is the formal definition: an observable $o \in C$

is *value definite* in the context C under v if $v(o,C)$ is defined; otherwise o is *value indefinite* in C. If o is value definite in all contexts $C \in \mathcal{C}$ for which $o \in C$ then we simply say that o is value definite under v. The set O is *value definite* under v if every observable $o \in O$ is value definite under v.

Non-contextuality corresponds to the classical notion that the value obtained via measurement is independent of other compatible observables measured alongside it. Formally, an observable $o \in O$ is *non-contextual* under v if for all contexts $C, C' \in \mathcal{C}$ with $o \in C, C'$ we have $v(o,C) = v(o,C')$; otherwise, v is *contextual*. The set of observables O is *non-contextual* under v if every observable $o \in O$ which is not value indefinite (i.e. value definite in *some* context) is non-contextual under v; otherwise, the set of observables O is *contextual*.

To be in agreement with quantum mechanics we restrict the assignment functions to admissible ones: v is *admissible* if the following hold for all $C \in \mathcal{C}$: a) if there exists an $o \in C$ with $v(o,C) = 1$, then $v(o',C) = 0$ for all $o' \in C \setminus \{o\}$, b) if there exists an $o \in C$ such that $v(o',C) = 0$ for all $o' \in C \setminus \{o\}$, then $v(o,C) = 1$.

V. PHYSICAL ASSUMPTIONS

We are now ready to list the physical assumptions need in what follows.

A *value indefinite quantum experiment* is an experiment in which a particular value indefinite observable in a standard (von Neumann type) quantum mechanics is measured, subject to the following assumptions **(A1)–(A5)** (for a detailed motivation we refer to [1]).

We exclude interpretations of quantum mechanics, such as the many-worlds interpretation, where there is no unique "result" of a measurement.

> **(A1) Measurement assumption.** *Measurement yields a physically meaningful and unique result.*

We restrict the set of assignments to those which agree with quantum mechanics.

> **(A2) Assignment assumption.** *The assignment function v is a* faithful *representation of a realisation r_ψ of a state $|\psi\rangle$, that is, the measurement of observable o in the context C on the physical state r_ψ yields the result $v(o,C)$ whenever o has a definite value under v.*

We assume a classical-like behaviour of measurement: the values of variables are intrinsic and independent of the device used to measure them.

> **(A3) Non-contextuality assumption.** *The set of observables $\mathcal{O}$ is non-contextual.*

The following assumption reflects another agreement with quantum mechanics.

> **(A4) Eigenstate assumption.** *For every (normalised) quantum state $|\psi\rangle$ and faithful assignment function v, we have $v(P_\psi, C) = 1$ and $v(P_\phi, C) = 0$, for any context $C \in \mathcal{C}$, with $P_\psi, P_\phi \in C$.*

In the next assumption we adopt a method to determine a class of value definite observables. The motivation is the notion of "element of physical reality" described by Einstein, Podolsky and Rosen in [8, p. 777]:

> *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality* [which equates to the notion of a definite value, possibly contextual] [(*e.p.r.*)] *corresponding to this physical quantity.*

The next assumption is a weak form of e.p.r. in which *prediction is certain* (not only with probability one) and, *given by some function which can be proved to be computable*.

> **(A5) Elements of physical reality (e.p.r.) assumption.** *If there exists a computable function $f : \mathbf{N} \times \mathcal{O} \times \mathcal{C} \to B$ such that for infinitely many $i \geq 1$, $f(i, o_i, C_i) = x_i$, then there is a definite value associated with o_i at each step* [i.e., $v_i(o_i, C_i) = f(i, o_i, C_i)$].

To use the e.p.r. assumption we need *to prove* the existence of a computable function f such that for infinitely many $i \geq 1$, $f(i, o_i, C_i) = x_i$.

VI. THE KOCHEN-SPECKER THEOREM

Can projection observables be value definite and non-contextual? The answer is negative.

Theorem VI.1 (Kochen-Specker theorem). *If $n > 2$ there exists a set of projection observables $\mathcal{O}$ on $\mathbb{C}^n$ and a set of contexts over $\mathcal{O}$ such that there is no admissible assignment function v under which $\mathcal{O}$ is both non-contextual and value definite.*

Kochen-Specker theorem [10] is a famous result showing a contradiction between two basic assumptions of a hypothetical hidden variable theory intended to reproduce the results of quantum mechanics: a) all hidden variables corresponding to quantum mechanical observables have definite values at any given time, and b) the values of those variables are intrinsic and independent of the device used to measure them. The result is important in the debate on the (in)completeness of quantum mechanics creating by the EPR paradox [8].

Interestingly, the theorem, that is considered a topic in the foundations of quantum mechanics, with more philosophical flavour and little presence in main stream quantum mechanical textbooks, has actually an operational importance. Indeed, using the assumption **(A3)**, the Kochen-Specker theorem states that some projection observables have to be value indefinite.

Why should we care about a value indefinite observable? Because a way "to see" the randomness in quantum mechanics is by measuring such an observable. Of course, we need to be able to *certify* that a given observable is value indefinite. Unfortunately the theorem gives no indication which observables are value indefinite. We know that not all projection observables are value indefinite [1], but can we be sure that a specific observable is value indefinite observable? The following result from [1] answers this question in the affirmative:

Theorem VI.2 (Strong Kochen-Specker theorem)**.** *Let* $|a\rangle, |b\rangle \in \mathbb{C}^3$ *be unit vectors such that* $0 < |\langle a|b\rangle| \leq \frac{3}{\sqrt{14}}$. *Then there exists a set of projection observables* O *containing* P_a *and* P_b*, and a set of contexts* $\mathcal{C}$ *over* O*, such that there is no admissible assignment function under which* O *is non-contextual and* P_a*,* P_b *have the value 1.*

An operational form of the strong Kochen-Specker theorem capable of identifying a value indefinite observable is given by

Theorem VI.3 (Operational Kochen-Specker theorem)**.** *Let* $|\psi\rangle \in \mathbb{C}^3$ *be a quantum state describing a system. Also let* $|\phi\rangle \in \mathbb{C}^3$ *be any other state which satisfies* $\sqrt{\frac{5}{14}} \leq |\langle\psi|\phi\rangle| \leq \frac{3}{\sqrt{14}}$. *Then, assuming non-contextuality,* P_ϕ *cannot be assigned a definite value by a faithful assignment function.*

Theorem VI.3 allows us to identify and then measure a value indefinite observable, a crucial point in what follows.

VII. QUANTUM RANDOMNESS

A *value indefinite quantum experiment* is an experiment in which a particular value indefinite observable in a standard (von Neumann type) quantum mechanics is measured, subject to the following assumptions (for more motivation we refer to [1]).

Consider a system in which a value indefinite quantum experiment is prepared, measured, rinsed and repeated ad infinitum. The infinite sequence $\mathbf{x} = x_1 x_2 \ldots$ obtained by concatenating the outputs of these measurements is called *value indefinite quantum random sequence*, shortly, *quantum random sequence*.

In [4] it was proved that *every unbiased, that is, 0 and 1 have been produced with equal probabilities, quantum random sequence is bi-immune*. In [1] the result was improved by removing the un-biassing assumption:

Theorem VII.1 (Strong incomputability theorem)**.** *Assume* **(A1)–(A5)** *for* $\mathbb{C}^3$. *Then, every quantum random sequence is bi-immune, that is, every Turing machine cannot compute exactly more than finitely many bits of the sequence.*

Bi-immunity assures that any adversary can be sure of no more than finitely many exact values—guessed or computed—of any given quantum random sequence. This is indeed a good certificate of quality for this type of quantum randomness.

VIII. PREDICTION BY OMISSION

In this section we identify a simple but general type of correlation, and its corresponding prediction, obtained indirectly, through *omission*.

A standard correlation is given by some explicit pattern or relation. For example, the correlation "every even bit is 0" fixes a specific value for even positions. The correlation "every even bit is equal to its predecessor" does not fix any values, but stipulates that the values on even positions are equal to the values on odd ones, whatever those may be.

Correlations are interesting because they reveal *patterns* which are useful for *prediction*. In the first example, the prediction is clear; in the second example the prediction rule is "the value on the even position is the value on the predecessor (odd) position".

If without knowing any bit of a sequence $\mathbf{x}$ *one can* prove *that a particular string* w *is not a* *prefix of the sequence* $\mathbf{x}$*, then we say that* $\mathbf{x}$ **omits the string** w. This definition, which requests *a proof*, will be used in conjuction with the e.p.r. assumption in Section VII.

Lemma VIII.1 (Omission Lemma)**.** *For every string w and every sequence* $\mathbf{x}$*, if* $\mathbf{x}$ *omits the string w, then* $\mathbf{x}$ *is not a quantum random sequence.*

Proof. Assume by contradiction that the quantum random sequence $\mathbf{x}$ omits the string $w = w_1 w_2 \cdots w_k$, $k \geq 1$. Assume that measuring $k-1$ times the value indefinite observable of the quantum experiment producing $\mathbf{x}$ we obtain independently the bits $w_1, w_2, \cdots, w_{k-1}$. What is the result of the next measurement? Because by hypothesis $\mathbf{x}$ omits the string w, we have a *proof* stating—before the process of measuring—that the next bit cannot be w_k, hence it should be $1 - w_k$. Value indefiniteness is violated, hence the bits $w_1, w_2, \cdots, w_{k-1}$ cannot be obtained as the result of the first $k-1$ measurements. Repeating again the reasoning we deduce that the bit w_1 cannot be obtained, hence a contradiction. □

At a first glance the Omission Lemma seems rather weak, as it identifies just one correlation. What power can have a single correlation for an infinite sequence?

Corollary VIII.2. *For every string w and every sequence* $\mathbf{x}$*, if* $\mathbf{x}$ *omits the string w, then* $\mathbf{x}$ *omits every string wu, for all $u \in B^*$.*

Proof. Indeed, if for some $u \in B^*$, it is false that $\mathbf{x}$ omits wu, then is false that $\mathbf{x}$ omits w, a contradiction. □

Corollary VIII.2 states that a sequence which omits a strings omits infinitely many strings. More precisely, if $\mathbf{x}$ omits w, then $\mathbf{x}$ omits an *infinite computable set of strings*. Indeed, let $w = w_1 w_2 \cdots w_k$ and let $F : B^* \to B$ be the computable function defined by

$$F(w_1 w_2 \cdots w_k u_1 \cdots u_t) = 1 - u_t,$$

for every $u_1 \cdots u_t \in B^*$.

The computable function $f : \mathbf{N} \times O \times \mathcal{C} \to B$ such that for every t, $f(k+t, o_{k+t}, C_{k+t}) = F(w_1 w_2 \cdots w_k u_1 \cdots u_t) = x_{k+t+1}$ shows that by e.p.r. assumption, there is a definite value associated with o_{k+t} at each step $t = 1, 2, \ldots$: this contradicts the non-contextuality assumption via the Kochen-Specker theorem.

Corollary VIII.3. *For every string w there exists a quantum random sequence* $\mathbf{x}$ *having w as prefix.*

Proof. If the statement of the corollary is false, then there exists a string w such that every quantum random sequence $\mathbf{x}$ omits the string w, contradicting Lemma VIII.1. □

Corollary VIII.3 proves that a value indefinite quantum experiment has to produce sequences starting with any string (of any length), which is in accord with the quantum mechanical predictions; the difference is that here the *phenomenon is true not only with probability one, but with certainty*.

IX. QUALITATIVE PROPERTIES OF QUANTUM RANDOM SEQUENCES

Properties which do not depend on the probability distribution of the source of randomness are called *qualitative*. For example, the property of a sequence $\mathbf{x}$ to contain any string w infinitely many times (formally, there exist infinitely many strings $u \in B^*$ such that uw is a prefix of $\mathbf{x}$)—called *disjunctivity*—is qualitative [], but the stronger property expressed by the law of large numbers (1) is not. For example, writing in binary the sequence of primes $2,3,5,7,11,13,17,19\cdots$ we obtain the disjunctive sequence $10111011111011110110001\cdots$ for which the law of large numbers fails to be true [].

Corollary IX.1. *Every quantum random sequence is disjunctive.*

Proof. Let w be a string and let $\mathbf{x}$ be a quantum random sequence. If $\mathbf{x}$ does not contain w, then it follows that for every string u, $\mathbf{x}$ omits uw, which contradicts the Omission Lemma. □

Computability is another qualitative property: one cannot compute any bit of a quantum random sequence.

Corollary IX.2. *Let* $\mathbf{x}$ *be a quantum random sequence. Then the function* $f_{\mathbf{x}} : \mathbb{N}_+ \to B$ *defined by* $f_{\mathbf{x}}(n) = x_n$*, for all* $n \geq 1$*, is not computable.*

Proof. Assume that one can prove that the function $f_{\mathbf{x}}$ is computable. Then, the sequence $\mathbf{x}$ omits every string $f_{\mathbf{x}}(1)\cdots f_{\mathbf{x}}(n)(1-f_{\mathbf{x}}(n))$, for every $n \geq 1$, contradicting the Omission Lemma. □

Recall that a sequence $\mathbf{x}$ is bi-immune no algorithm can enumerate the correct values of infinitely many bits of the sequence. Formally, there exists no computable strictly increasing function $f : \mathbb{N}_+ \to \mathbb{N}_+ \times B$ such that a) $\Pi_1(f(n))$ is strictly increasing and b) for all $n \geq 1$, $x_{\Pi_1(f(n))} = \Pi_2(f(n))$.

Theorem IX.3 (ACCS Theorem [1]). *Every quantum random sequence is bi-immune.*

Proof. Let us assume that $\mathbf{x}$ is a quantum random sequence which is not bi-immune, that is, one can prove the existence of a computable function f with the above properties a) and b). Then $\mathbf{x}$ omits every string of length $\Pi_1(f(n)) > 1$ whose last bit is $1 - \Pi_2(f(n))$, contradicting the Omission Lemma. □

Theorem IX.3 exploits the fact that some values of the sequence $\mathbf{x}$ are fixed in advanced, so predictible. Here is an example of a use of the Omission Lemma for a correlation in which no bit has a fixed value.

Example IX.4. *No quantum random sequence can be of the form $x_1x_1x_2x_2\ldots x_ix_i\cdots$, for any arbitrary sequence $\mathbf{x} = x_1x_2\ldots$.*

Proof. Let $\mathbf{x}$ be an arbitrary sequence and assume that the sequence $x_1x_1x_2x_2\ldots x_ix_i\ldots$ was obtained by a value indefinite quantum experiment. Clearly, this sequence omits the strings 10 and 01, contradicting again the Omission Lemma. □

Note that in both Theorem IX.3 and Example IX.4, a class of sequences is proved to be impossible to be obtained via a value indefinite quantum experiment. What set of correlations are prohibited from any quantum random sequence by the Omission Lemma? In particular, can we exclude sequences which do not obey the law of large numbers (1)?

X. QUANTITATIVE PROPERTIES OF QUANTUM RANDOM SEQUENCES

Consider the set of correlations $\mathcal{C}$ defined by "$\mathbf{x}_{2^k} = 0$, for some $k \geq 1$": they are an example of correlations contradicting bi-immunity. There are lots of sequences not having the correlations $\mathcal{C}$: infinitely many are computable, like the sequence $\mathbf{a}$ in Section III, and infinitely many are incomputable. To test whether a sequence $\mathbf{x}$ is $\mathcal{C}$–random we can check whether for all $i < n$ we have $\mathbf{x}_{2^i} = 1$. If this is not the case for a given pair $i < n$, then we know that $\mathbf{x}$ is not $\mathcal{C}$–random. In the opposite case, we cannot say anything for sure because only a finite prefix of $\mathbf{x}$ has been tested, but with confidence level of $1 - 2^{-n}$ we can "believe" that $\mathbf{x}$ is $\mathcal{C}$–random. When the test cannot find any $i < n$ with $\mathbf{x}_{2^i} = 0$, for larger and larger n, the probability of our "belief" gets higher and higher. The natural probability for this phenomenon is the probability distribution of value indefinite experiment. This leads to the last assumption:

(A6) **Probability distribution assumption.** *The value indefinite experiment is un-biassed, i.e. it produces 0 and 1 with equal probabilities.*

The Lebesgue measure—which models the probability distribution assumption—of the set of sequences for which the test indicates that are $\mathcal{C}$–random with confidence $1-2^{-n}$ is smaller that $2^{-\lfloor n \rfloor}$, which converges to 0 as n tends to infinity; so most sequences are $\mathcal{C}$–random.

The correlations $\mathcal{C}$ are weak, hence many sequences which are intuitively atypical are also $\mathcal{C}$–random: for example, the sequence $\mathbf{a}$. To obtain a class of sequences having a higher quality of randomness we need to consider more and more "subtle" sets of correlations; in this process the quality of the corresponding $\mathcal{C}$–random sequences increases. By defining randomness tests in terms of simple constructive subsets of sequences of smaller and smaller Lebesgue measure, Martin-Löf [12] was able to define a set of correlations $\mathcal{C}$ for which the corresponding $\mathcal{C}$–random sequences have most (but, by Ramsey theory [9], not **all**) intuitively desirable randomness properties.

A non-empty c.e. set $T \subset X^* \times \mathbb{N}_+$ is a *Martin-Löf (randomness) test* if

(m1) $T_{m+1} \subseteq T_m$, for all $m \geq 1$,

(m2) $\#(B^n \cap T_m) < 2^{n-m}$, for all $n,m \geq 1$,

(m3) for all $m \geq 1$, and $u \in T_m$, $u \sqsubset v$, then $v \in T_m$.

The Lebesgue measure of the set $T_m B^\infty$ is smaller than 2^{-m}, i.e. $\mu(T_m B^\infty) \leq 2^{-m}$; this implies that $\lim_{n\to\infty} \mu(T_m B^\infty) = 0$, effectively.

A class of sequences $S \subset B^\infty$ is *Martin-Löf null* if there exists a Martin-Löf test T such that $S \subset \bigcap_{m\geq 1} T_m B^\infty$.

Here are some examples of Martin-Löf null classes of sequences.

Example X.1 ([3])**.** *The law of large numbers corresponds to the class of sequences* $\{\mathbf{x} \in B^\infty \mid \lim_{n\to\infty}(\mathbf{x}_1 + \mathbf{x}_2 + \cdots + \mathbf{x}_n)/n = 1/2\}$ *which is a Martin-Löf null class.*

Example X.2. *Every non-bi-immune sequence is contained in a Martin-Löf null class.*

Proof. Let $\mathbf{x}$ be a sequence which is not bi-immune, i.e. there exists an infinite c.e. set $B \subset \mathbb{N}_+ \times B$ such that for every $(n,i) \in B$ we have $\mathbf{x}(n) = i$. Let $e\colon \mathbb{N}_+ \to \mathbb{N}_+ \times \{0,1\}$ be an injective computable function which enumerates B, i.e. $e(\mathbb{N}_+) = B$. Define the computable function $first$: $\mathbb{N}_+ \to \mathbb{N}_+$ by

$$first(k) = \max\{\Pi_1(e(1)), \ldots, \Pi_1(e(k))\},$$

and the computable set

$$T(B) = \{(z_1 z_2 \ldots z_{first(k)}, k) \in B^* \times \mathbb{N}_+ \mid 1 \leq i \leq k, z_{\Pi_1(e(i))} = \Pi_2(e(i))\}.$$

The set $T(B)$ is a Martin-Löf test and $\mathbf{x}$ is contained in the Martin-Löf null class $\bigcap_{k \in \mathbb{N}_+}[T(B)_k]$ as $\mathbf{x}\restriction_{first(k)} \in T(B)_k$. □

Example X.3. *Every computable sequence is contained in a Martin-Löf null class.*

Proof. Every computable sequence is bi-immune, so the result follows from Exemple X.2. □

A celebrated result is:

Theorem X.4 (Martin-Löf,[12]). *The union of all Martin-Löf null classes* $\mathfrak{ML}\text{-}\mathfrak{null}$ *is a Martin-Löf null class. In particular, the set of Martin-Löf random sequences—which is equal to the complement of* $\mathfrak{ML}\text{-}\mathfrak{null}$*—has effective Lebesgue measure one.*

In contrast with the classical Lebesgue measure theory, not all singletons Martin-Löf null:

Example X.5. *There exist sequences* $\mathbf{x}$ *such that the singleton class* $\{\mathbf{x}\}$ *is not Martin-Löf null.*

Proof. By Theorem X.4, for every $\mathbf{x} \notin \mathfrak{ML}\text{-}\mathfrak{null}$, $\{\mathbf{x}\}$ is not is Martin-Löf null. □

Theorem X.6. *No sequence produced by an un-biassed value indefinite quantum experiment can belong to any infinite Martin-Löf null set, in particular, it is Martin-Löf random.*

Proof. Assume that $\mathbf{x}$ is a quantum random sequence produced by un-biassed experiment and $\mathbf{x}$ belongs to an infinite Martin-Löf null set T. It follows that $\mathbf{x} \in \bigcap_{m \geq 1} T_m B^\infty$. For every $n \geq 1$ there exists $m_n > n$ such that $\mathbf{x}\restriction_{m_n} \in B^{m_n} \cap T_m$ and because T is a Martin-Löf test $\#(B^{m_n} \cap T_m) < 2^{m_n - n} < 2^{m_n}$, which shows that for every $n > 0$, $\mathbf{x}$ omits at least one string of length $m_n > n$, a contradiction according with the Omission Lemma. □

To use the Omission Lemma we need to use show that a single string is omitted (which, according to Corollary VIII.2, implies that an infinite computable set of strings is omitted): the above proof shows that the quantum random sequence omits infinitely many strings, for each of which Corollary VIII.2 applies.

Assume that $\mathbf{x}$ is a quantum random sequence belonging to an infinite Martin-Löf null set T enumerated by the computable function $t : \mathbb{N}_+ \to B^* \times \mathbb{N}$, i.e. $T = t(\mathbb{N}_+)$. For every positive integer n there exists an integer $m_n > n$ such that $\mathbf{x}\restriction_{m_n} \in T_n$. The condition $m_n > n$ comes from the inequality $\mu(T_n B^\infty) \leq 2^{-n}$, as every $s \in T_n$ has to be longer than n, $|s| > n$. Re-writing the above condition in terms of the computable function t we get: for every positive integer n there exist an integer $m_n > n$ and i_n such that

$$\mathbf{x}\restriction_{m_n} = \Pi_1(t(i)) \text{ and } \Pi_2(t(i_n)) = n. \tag{2}$$

We conclude that every quantum random sequence $\mathbf{x}$ *has to obey* the set of correlations (2). Are the correlations (2) of Ramsey's type, i.e. they have to be satisfied by *every sequence*, not only by quantum sequences? The answer is negative as the set of sequences having correlations of the form (2) has effective measure zero by Theorem X.4, far from being the set of all sequences.

Corollary X.7. *Every sequence produced by an un-biassed value indefinite quantum experiment satisfies the law of large numbers.*

Proof. Use Example X.1 and Theorem X.6. □

XI. IMPERFECT QRNG

TODO: as in [1].

---

[1] A. A. Abbott, C.S. Calude, J. Conder, K. Svozil. Strong Kochen-Specker theorem and incomputability of quantum randomness, *Physical Review A* 86, 6 (2012), DOI: 10.1103/PhysRevA.00.002100.

[2] A. Abbott, C. S. Calude, K. Svozil. A quantum random number generator certified by value indefiniteness, *Mathematical Structures in Computer Science*, 2013, to appear.

[3] C. S. Calude. *Information and Randomness: An Algorithmic Perspective*, Springer-Verlag, Berlin, 2002 (2nd Edition).

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

[5] J. Cederlof, J.-A. Larsson. Security aspects of the authentication used in quantum cryptography, *IEEE Transactions on Information Theory*, 54, 4, (2008), 1735–1741.

[6] D. G. Champernowne. The construction of decimals normal in the scale of ten, *J. London Math. Soc.* 8 (1933), 254-260.

[7] R. Downey, D. Hirschfeldt. *Algorithmic Randomness and Complexity*, Springer, Heidelberg, 2010.

[8] A. Einstein, B. Podolsky, N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* 47 (1935), 777–780.

[9] R. Graham, J. H. Spencer. Ramsey theory, *Scientific American* 262 no. 7 (1990), 112–117.

[10] S. Kochen, E. P. Specker. The problem of hidden variables in quantum mechanics, *Journal of Mathematics and Mechanics* 17 (1967), 59–87.

[11] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination, *Nat. Photon* 4, 10 (2010), 686–689. Supplementary information `http://www.nature.com/nphoton/journal/v4/n10/abs/nphoton.2010.214.html`.

[12] P. Martin-Löf. The definition of random sequences, *Inform. and Control* 9(1966), 602-619.

[13] A. Soifer. Ramsey theory before Ramsey, prehistory and early history: An essay, in A. Soifer (ed.), *Ramsey Theory: Yesterday, Today, and Tomorrow*, Springer, Progress in Mathematics 285, Berlin, 2011, 1–26.

[14] Conference on Lasers and Electro-Optic 2013, `http://www.cleoconference.org/home/news-and-press/cleo-press-releases/cleo-2013-the-premier-international-laser-and-elec/`.

[15] True randomness demonstrated, `http://www.nature.com/nature/journal/v464/n7291/edsumm/e1`