Martin-Löf random quantum states

View Online   Export Citation   CrossMark

André Nies[1,a] (iD) and Volkher B. Scholz[2,a]

AFFILIATIONS

[1] School of Computer Science, The University of Auckland, Auckland, New Zealand
[2] ETH and Belimo, Zürich, Switzerland

[a] Electronic addresses: andre@cs.auckland.ac.nz and scholz@phys.ethz.ch

ABSTRACT

We extend the key notion of Martin-Löf randomness for infinite bit sequences to the quantum setting, where the sequences become states of an infinite dimensional system. We prove that our definition naturally extends the classical case. In analogy with the Levin-Schnorr theorem, we work toward characterizing quantum ML-randomness of states by incompressibility (in the sense of quantum Turing machines) of all initial segments.

Published under license by AIP Publishing. https://doi.org/10.1063/1.5094660

I. INTRODUCTION

A. Algorithmic theory of randomness in the classical setting

An infinite sequence of classical bits can be thought of as random if it satisfies no exceptional properties. Examples of exceptional property are that every other bit is 0 and that all initial segments have more 0s than 1s. An infinite sequence of fair coin tosses has neither of the two properties.

Infinite bit sequences form the so-called Cantor space $2^{\mathbb{N}}$, which is equipped with a natural compact topology, and the uniform measure which makes the infinitely many coin tosses independent and fair. Recall that a subset of $2^{\mathbb{N}}$ is defined to be *null* if it is contained in $\bigcap_m G_m$ for a sequence of open sets G_m with measure tending to 0. An exceptional property then corresponds to a null set in $2^{\mathbb{N}}$.

Since no sequence can actually avoid all the null sets, one has to restrict the class of null sets that can be considered. One only allows null sets that are effective, i.e., can be described in an algorithmic way. The possible levels of effectiveness one can choose determine a hierarchy of formal randomness notions. Such notions are studied, for instance, in the books.[9,25] In recent work, the algorithmic theory of randomness has been connected to mathematical fields such as ergodic theory and set theory.[23,15,20,21]

Martin-Löf (ML) randomness, introduced in Ref. 17, is a central algorithmic randomness notion. Roughly speaking, a bit sequence Z is ML-random if it is in no null set $\bigcap_{m\in\mathbb{N}} G_m$, where G_m are effectively open uniformly in m and the uniform measure of G_m is at most 2^{-m}. This notion is central because there is a universal test and because ML-randomness of an infinite bit sequence can be naturally characterized by an incompressibility condition on the initial segments of the sequence (Levin-Schnorr theorem). Details have been given below.

B. The quantum setting

Our main goal is to develop an algorithmic theory of randomness for infinite sequences of quantum bits. This poses two challenges.

The first challenge is to provide a satisfying mathematical model for such sequences. This is not as straightforward as in the classical case: deleting one qubit from a system of finitely many entangled qubits (e.g., the EPR state, which describes two entangled photons) creates a mixed state, namely, a statistical superposition of possibilities for the remaining qubits. So one actually studies states of a system that can be interpreted as statistical superpositions of infinite sequences of quantum bits (qubits). Such states have been considered in theoretical physics in the form of half-infinite spin chains (e.g., a linear arrangement of hydrogen atoms with the electron in the basic or the excited state).

The usual mathematical approach (e.g., Refs. 7, 6, and 2) to deal with such statistical superpositions is as follows. The sequences of qubits are modeled by coherent sequences $\langle \rho_n \rangle_{n \in \mathbb{N}}$ of density matrices. We have $\rho_n \in M_n$, where M_n is the algebra of $2^n \times 2^n$ matrices over $\mathbb{C}$. The idea is that ρ_n describes the first n qubits. Infinite qubit sequences are states (that is, positive functionals of norm 1) of a certain C^*-algebra M_{2^∞}, the direct limit of the matrix algebras M_n.

The second challenge is the absence of measure in the quantum setting. We will use instead the unique tracial state τ on M_∞ as a noncommutative analog of the uniform measure. For a projection $p \in M_n$, one has $\tau(p) = 2^{-n} \dim \texttt{rg}(p)$. The analog of an effectively open set in Cantor space is now a computable increasing sequence $G = \langle p_n \rangle_{n \in \mathbb{N}}$ of projections, $p_n \in M_n$, and one defines $\tau(G) = \sup_n \tau(p_n)$. Based on this, we will introduce our main technical concept, a quantum version of ML-tests.

C. Overview of the paper

Section II provides the necessary preliminaries on *finite* sequences of qubits, as well as on density matrices, which describe statistical superpositions of qubit sequences of the same length. We also review the mathematical model for states that embody infinite sequences of qubits.

In Sec. III, we introduce quantum Martin-Löf tests. We show that there is a universal such test. Every infinite sequence of classical bits can be seen as a state of the C^*-algebra M_{2^∞}. We show that for such a sequence, quantum ML-randomness coincides with the usual ML-randomness. So our notion naturally extends the classical one.

The Levin-Schnorr theorem (Levin[16] and Schnorr[28]) characterizes ML-randomness of a bit sequence Z by the growth rate of the initial segment complexity $K(Z \upharpoonright_n)$ (here, $Z \upharpoonright_n$ denotes the string consisting of the first n bits and K denotes a version of Kolmogorov complexity where the set of descriptions that a universal machine can use as inputs has to be prefix free). In Sec. IV, we work toward a potential quantum version of this important result. This would mean that quantum Martin-Löf random states are characterized by having initial segments of a fast growing quantum Kolmogorov complexity. The actual formulation of our result corresponds to the Gács-Miller-Yu theorem[12,18] which uses plain Kolmogorov complexity C, rather than the original Levin-Schnorr theorem, for reasons related to different properties of classical and quantum Turing machines.[4]

We note that there has been an earlier application of notions from computability theory to spin chains. Wolf, Cubitt, and Perez-Garcia[8] studied undecidability in the quantum setting. They constructed Hamiltonians on square lattices with associated ground states which radically change behavior as the system size grows. For example, while being a product state for small system sizes, it becomes entangled for large sizes.[1] Furthermore, based only on initial segments of the sequence, it is computationally impossible to predict whether this effect happens. The states we consider here are defined on a spin chain rather than on a two-dimensional lattice and are also not constrained to be ground states of local Hamiltonians. However, they share similar features in the sense of possessing unpredictable behavior as the system size grows.

II. PRELIMINARIES

A. Quantum bits

A classical bit can be in states 0, 1. A qubit is a physical system with two possible classical states: for instance, the polarization of photon horizontal/vertical and a hydrogen atom in the ground or the first excited state. A qubit can be in a superposition of the two classical states $\alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$. A measurement of a qubit with respect to the standard basis $|0\rangle$, $|1\rangle$ yields 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$.

B. Finite sequences of quantum bits

The state of a physical system is represented by a vector in a finite dimensional Hilbert space A. For vectors $a, b \in A$, $\langle a|b \rangle$ denotes the inner product of vectors a, b, which is linear in the *second* component and antilinear in the first. For systems represented by Hilbert spaces A, B, the tensor product $A \otimes B$ is a Hilbert space that represents the combined system. One defines an inner product on $A \otimes B$ by $\langle a \otimes b | c \otimes d \rangle = \langle a|c \rangle \langle b|d \rangle$.

Mathematically, a qubit is simply a unit vector in $\mathbb{C}^2$. The state of a system of n qubits is a unit vector in the tensor power

$$\mathcal{H}_n := (\mathbb{C}^2)^{\otimes n} = \underbrace{\mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2}_{n}.$$

We denote the standard basis of $\mathbb{C}^2$ by $|0\rangle$, $|1\rangle$. The standard basis of $\mathcal{H}_n$ consists of vectors

$$|a_0 \ldots a_{n-1}\rangle := |a_0\rangle \otimes \cdots \otimes |a_{n-1}\rangle,$$

where $\sigma = a_0 \ldots a_{n-1}$ is an n-bit string. While the usual notation for $|a_0 \ldots a_{n-1}\rangle$ in quantum physics is $|\sigma\rangle$, for brevity, we will often write $\underline{\sigma}$. The state of the system of n qubits is a unit vector $\mathcal{H}_n$ and hence a certain linear superposition of these basis vectors. For example, for $n = 2$, the EPR (or "maximally entangled") state is $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

C. Mixed states and density operators

With each state $|\psi\rangle$ (a unit vector in $\mathcal{H}_n$), we associate, and often identify, the linear form $|\psi\rangle\langle\psi|$ on $\mathcal{H}_n$ given by $|\phi\rangle \mapsto |\psi\rangle\langle\psi|\phi\rangle$. A *mixed state* is a convex linear combination $\sum_{i=1}^{2^n} p_i |\psi_i\rangle\langle\psi_i|$ of pairwise orthogonal states ψ_i. In this context, a state $|\psi\rangle$ (identified with $|\psi\rangle\langle\psi|$) is called *pure*.

Recall that for an operator S on a finite dimensional Hilbert space A, the trace $\mathrm{Tr}(S)$ is the sum of the eigenvalues of S (counted with multiplicity). A Hermitian operator is called positive if all eigenvalues are non-negative. A mixed state corresponds to a positive operator S on $\mathcal{H}_n$ with $\mathrm{Tr}(S) = 1$ as one can see via the spectral decomposition of S.

A C^*-algebra is a subalgebra of the bounded operators on some Hilbert space closed under taking the adjoint and topologically closed in the operator norm. We let

$$M_{2^k} = \mathrm{Mat}_{2^k}(\mathbb{C})$$

denote the C^*-algebra of $2^k \times 2^k$ matrices over $\mathbb{C}$ (identified with operators on $\mathbb{C}^{2^k}$). A *density operator* (or density matrix) in M_{2^k} is a positive operator in M_{2^k} with trace 1. The states $\rho \in \mathcal{S}(M_{2^k})$ can be identified with the density operators S on $\mathcal{H}_k$ to a state ρ corresponds the unique density operator S such that

$$\rho(X) = \mathrm{Tr}(SX) \text{ for each } X \in M_{2^k}. \tag{1}$$

D. Embeddings between matrix algebras

We view $\mathcal{H}_{n+1}$ as the tensor product $\mathcal{H}_n \otimes \mathbb{C}^2$. Then, $M_{2^{n+1}}$ is naturally isomorphic to $M_{2^n} \otimes M_{2^1}$. We view the indices of matrix entries as numbers written in "reverse binary," i.e., with the most significant digit written on the right. Thus, a matrix entry is indexed by a pair of strings σ, τ of the same length, and a matrix in $M_{2^{n+1}}$ has the form

$$A = \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix},$$

where each $A_{i,k} = (a_{\sigma i, \tau k})_{|\sigma|=|\tau|=n}$ is in M_{2^n}. We have embeddings $M_{2^n} \to M_{2^{n+1}}$ given by

$$A \mapsto A \otimes I_2 = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}. \tag{2}$$

Note that the embeddings preserve the operator norm.

E. Partial trace operation

For each n, there is a unique linear map $T_n : M_{2^{n+1}} \to M_{2^n}$, called the partial trace operation, such that $T_n(R \otimes S) = R \cdot \mathrm{Tr}(S)$ for each $R \in M_{2^n}$ and $S \in M_{2^1}$. Intuitively, this operation corresponds to deleting the last qubit, for instance, $T_1(|10\rangle\langle10|) = |1\rangle\langle1|$.

Remark 2.1. Consider again the EPR state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, now viewed as the operator $\beta = \frac{1}{2}(|00\rangle + |11\rangle)(\langle00| + \langle11|)$ in M_2. While this state is pure, $T_1(\beta) = \frac{1}{2}(|0\rangle\langle0| + |1\rangle\langle1|)$ is a properly mixed state.

One can provide an explicit description of the partial trace operation T_n as follows. $\mathcal{H}_{n+1}$ has as a base $|\sigma r\rangle$, σ a string of n bits, r a bit. For a $2^{n+1} \times 2^{n+1}$ matrix $A = (a_{\sigma r, \tau s})_{|\sigma|,|\tau|=n, r,s \in \{0,1\}}$, $T_n(A)$ is given by the $2^n \times 2^n$ matrix

$$b_{\sigma,\tau} = a_{\sigma 0, \tau 0} + a_{\sigma 1, \tau 1}. \tag{3}$$

It is easy to check that if A is a density matrix, then so is $T_n(A)$.

F. Direct limit of matrix algebras and tracial states

The so-called CAR algebra M_{2^∞} is the direct limit of the M_{2^k} under the norm-preserving embeddings in (2). Thus, M_{2^∞} is the norm completion of the union of the M_{2^n}, seen as a $*$-algebra. Clearly, M_{2^∞} is a C^*-algebra.

A *state* on a C^*-algebra M is a positive linear functional $\rho : M \to \mathbb{C}$ that sends the unit element of M to 1 (this implies that $\|\rho\| = 1$). To be positive means, $x \geq 0 \to \rho(x) \geq 0$.

A state ρ is called *tracial* if $\rho(ab) = \rho(ba)$ for each pair of operators a, b. On M_{2^n}, there is a unique tracial state τ_n given by $\tau_n(a) = 2^{-n}\mathrm{Tr}(a) = 2^{-n}\sum_{|\sigma|=n} a_{\sigma,\sigma}$. The corresponding density matrix is $2^{-n}I_{2^n}$ (i.e., it has 2^{-n} on the diagonal and 0 elsewhere). Note that the states τ_n are compatible with the embeddings $M_{2^n} \to M_{2^{n+1}}$. This yields a tracial state τ on M_{2^∞}, which is unique as well.

G. Quantum Cantor space

The quantum analog of Cantor space is $\mathcal{S}(M_{2^\infty})$, the set of states of the C^*-algebra M_{2^∞}. The space $\mathcal{S}(M_{2^\infty})$ is endowed with a convex structure and is compact in the weak $*$ topology [the coarsest topology that makes the application maps $\rho \mapsto \rho(x)$ continuous] by the Banach-Alaoglu theorem. The following is well known but hard to reference in this form.

Fact 2.2. *A state $\rho \in \mathcal{S}(M_{2^\infty})$ corresponds to a sequence $\langle \rho_n \rangle_{n\in\mathbb{N}}$, where ρ_n is a density matrix in M_{2^n} and which is coherent in the sense that taking the partial trace of ρ_{n+1} yields ρ_n.*

Proof. First, let $\rho \in \mathcal{S}(M_{2^\infty})$. Let ρ_n be the state which is the restriction of ρ to M_{2^n} (later on, we will use the notation $\rho \upharpoonright_n$). Let S_n be the density matrix on M_{2^n} corresponding to ρ_n according to (1).

Claim 2.3. $T_n(\rho_{n+1}) = \rho_n$.
To see this note that a brief calculation using (3) shows that for each $A \in M_{2^n}$,

$$\mathsf{Tr}\left(S_{n+1}\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}\right) = \mathsf{Tr}\left(T_n(S_{n+1})A\right).$$

We also have $\rho_{n+1}(A \otimes I_2) = \rho_n(A)$ by definition of ρ_n. Therefore, $T_n(S_{n+1}) = S_n$ by the uniqueness of the density matrix for ρ_n.

Conversely, given a sequence (ρ_n) of states on M_{2^n} such that $T_n(\rho_{n+1}) = \rho_n$, there is a unique $\rho \in \mathcal{S}(M_{2^\infty})$ such that ρ_n is the restriction of ρ to M_{2^n} for each n. To see this, first one defines a bounded functional $\widetilde{\rho}$ on the $*$-algebra $\bigcup_n M_{2^n}$ that extends each ρ_n. Then, one extends $\widetilde{\rho}$ to a state ρ on M_{2^∞} using that $\widetilde{\rho}$ is continuous. □

We need to allow mixed states as sequence entries when we develop an analog of infinite bit sequences for qubits: as discussed in Remark 2.1, the EPR state $\beta \in M_2$ is a pure state which turns into the mixed state after taking the partial trace. The following example may be instructive: letting $\rho_{2n} = \beta^{\otimes n}$ and $\rho_{2n+1} = \rho_{2n} \otimes \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$, we obtain a state such that the even initial segments are pure and the odd ones are mixed.

Remark 2.4. Suppose that all ρ_n are in diagonal form, and hence the entries of the corresponding matrices are in $[0, 1]$. For each σ, we can interpret $a_{\sigma,\sigma}$ as the probability that σ is an initial segment of a bit sequence: by (3), we have $a_{\sigma,\sigma} = a_{\sigma 0,\sigma 0} + a_{\sigma 1,\sigma 1}$. In other words, $\rho \in \mathcal{S}(M_{2^\infty})$ with all ρ_n in diagonal form correspond to the probability measures on $2^\mathbb{N}$. The tracial state τ defined in Subsection II F corresponds to the uniform measure.

One can now view an infinite sequence of classical bits $Z \in 2^\mathbb{N}$ as a state in $\mathcal{S}(M_{2^\infty})$, which corresponds to the probability measure concentrating on $\{Z\}$. For more detail, recall that the Hilbert space $\mathcal{H}_n$ has as a base the vectors $|\sigma\rangle$, for a string σ of n classical bits. A classical bit sequence Z corresponds to the state $(\rho_n)_{n\in\mathbb{N}}$, where the bit matrix $B = \rho_n \in M_{2^n}$ is given by $b_{\sigma,\tau} = 1 \Leftrightarrow \sigma = \tau = Z \upharpoonright_n$. For $\sigma = Z \upharpoonright_n$, ρ_n is the pure state $|\sigma\rangle\langle\sigma|$ on M_{2^n}.

H. Characterization of quantum Cantor space

Cantor space can be characterized as the projective (or inverse) limit of the discrete topological spaces X_n of n-bit strings with the maps $f_n: X_{n+1} \to X_n$ so that $f_n(\sigma r) = \sigma$, i.e., f_n removes the last bit. We now show that quantum Cantor space is a projective limit of the state sets of M_{2^n}.

By a *convex (topological) space*, we mean a topological space X with a continuous operation $F(\delta, a, b) = \delta a + (1 - \delta)b$, for $\delta \in [0, 1]$, $a, b \in X$, satisfying obvious arithmetical axioms such as $F(\delta, a, a) = a$. Clearly, $\mathcal{S}(M_{2^n})$ is a convex space. A map $g: X \to Y$ between convex spaces is called *affine* if $g(F(\delta, a, b)) = F(\delta, g(a), g(b))$ for each $a, b \in X$ and each δ. The *projective limit* of a sequence $\langle X_n \rangle$ of convex spaces with continuous affine maps $T_n: X_{n+1} \to X_n$, $n \in \mathbb{N}$ (called a diagram), is the convex space P of all $\rho \in \prod_n X_n$ such that $T_n(\rho(n + 1)) = \rho(n)$ for each n with the subspace topology and the canonical operation F.

Denote by $g_n: P \to X_n$ the map sending ρ to $\rho(n)$. The projective limit P is characterized up to affine homeomorphism by as a colimit from category theory: we have $T_n \circ g_{n+1} = g_n$ for each n and for any convex space A with continuous affine maps $f_n: A \to X_n$ such that $T_n \circ f_{n+1} = f_n$ for each n, there is a unique continuous affine map $f: A \to P$ such that $g_n \circ f = f_n$ for each n.

Proposition 2.5. *Consider the diagram consisting of $\mathcal{S}(M_{2^n})$ together with the partial trace maps $T_n: \mathcal{S}(M_{2^{n+1}}) \to \mathcal{S}(M_{2^n})$. Seen as a convex space, $\mathcal{S}(M_{2^\infty})$ is affinely homeomorphic to the projective limit of $\mathcal{S}(M_{2^n})$.*

Proof. Define $\widehat{g}_n: \mathcal{S}(M_{2^\infty}) \to \mathcal{S}(M_{2^n})$ by $\widehat{g}_n(\rho) = \rho \upharpoonright_{M_{2^n}}$. By Claim 2.3, $T_n \circ \widehat{g}_{n+1} = \widehat{g}_n$ for each n. It now suffices to verify the universal property for $\mathcal{S}(M_{2^\infty})$ together with the maps $\widehat{g}_n: \mathcal{S}(M_{2^\infty}) \to \mathcal{S}(M_{2^n})$. Suppose we are given a convex space A with continuous affine maps $f_n: A \to \mathcal{S}(M_{2^n})$ such that $T_n \circ f_{n+1} = f_n$ for each n. Let $f: A \to \mathcal{S}(M_{2^\infty})$ be the map such that $f(x) = \rho$, where ρ is the state determined as above by the sequence $\rho_n \in \mathcal{S}(M_{2^n})$ such that $\rho_n = f_n(x)$. Clearly f is affine. We show that f is continuous. A basic open set of $\mathcal{S}(M_{2^\infty})$ with its weak-$*$ topology has the form

$$U_{v,S} = \{\rho: \rho(v) \in S\},$$

where $v \in M_{2^\infty}$ and $S \subseteq \mathbb{C}$ are open. If $\rho \in U_{v,S}$, then there is $\varepsilon > 0$ such that the open ball $B_\varepsilon(\rho(v))$ is contained in S. Furthermore, there is $k \in \mathbb{N}$ and $w \in M_{2^k}$ such that $\|v - w\| < \varepsilon/2$. Since states have operator norm 1, this implies $|\rho(w) - \rho(v)| < \varepsilon/2$. Letting $S' = B_{\varepsilon/2}(\rho(v))$, we have $U_{w,S'} \subseteq U_{v,S}$.

So for continuity of f, it suffices to show that $f^{-1}(U_{w,S'})$ is open for any k, any $w \in M_{2^k}$ and open $S' \subseteq \mathbb{C}$. By the definition of f, we have $f^{-1}(U_{w,S'}) = f_k^{-1}(\{\theta \in \mathcal{S}(M_k): \theta(w) \in U_{w,S'}\})$. Since $\rho(w) = \rho \upharpoonright_{M_{2^k}} (w)$, $f^{-1}(U_{w,S'})$ is open by the hypothesis that $f_k: A \to \mathcal{S}(M_{2^k})$ is continuous. □

III. RANDOMNESS FOR STATES OF M_{2^∞}

Our main purpose is to introduce and study a version of Martin-Löf's randomness notion for states on M_{2^∞}, Definition 3.3. We begin by recalling the definition of Martin-Löf tests, phrased in such a way that it can be easily lifted to the quantum setting. A clopen (i.e., closed and open) set C in Cantor space can be described by a set F of strings of the same length k in the sense that $C = \bigcup_{\sigma \in F}\{Z: Za\sigma\}$ (note that k is not unique). A Σ_1^0 set $\mathcal{S}$ (or effectively open set) is a subset of Cantor space $2^\mathbb{N}$ given in a computable way as an ascending union of clopen sets. In more detail, we have $\mathcal{S} = \bigcup C_n$, where C_n is clopen, $C_n \subseteq C_{n+1}$, and a finite description of C_n can be computed from n. A Martin-Löf *test* is a uniformly computable sequence of Σ_1^0 sets $\langle G_m \rangle_{m \in \mathbb{N}}$ (i.e., $G_m = \bigcup_k C_k^m$, where the map sending a pair m, k to a description of the clopen set C_k^m is computable) such that $\lambda G_m \leq 2^{-m}$. Here, λ denotes the uniform measure, which Cyrilis obtained by viewing the kth bit as the result of the kth toss of a fair coin, where all the coin tosses are independent.

A sequence $Z \in 2^\mathbb{N}$ is Martin-Löf random if it passes all such tests in the sense that $Z \notin \bigcap_m G_m$. By the 1973 Levin-Schnorr theorem (see, e.g., Ref. 25, 3.2.9), this is equivalent to the incompressibility condition on initial segments that for some constant b, for each n, the prefix free Kolmogorov complexity of the first n bits of Z is at least $n - b$.

As an aside, if we add the restriction on tests that the measure of G_m is a computable real uniformly in m, we obtain the weaker notion of Schnorr randomness, now frequently used in the effective study of theorems from analysis, e.g., Ref. 27. This notion (as well as its variant, computable randomness) embodies an alternative paradigm of randomness, namely, that it is hard to predict the next bit from the previously seen ones.

In the following, we will use letters ρ, η for states on M_{2^∞}. We write $\rho \upharpoonright_n$ for the restriction of ρ to M_{2^n}, viewed either as a density matrix or a state of M_{2^n}. After introducing quantum ML-randomness in Definition 3.3, we will show that it ties in with the classical definition of ML-randomness. As mentioned above, any classical bit sequence defines a pure (product) quantum state of M_{2^∞}, by mapping the bits to the corresponding basis elements in the computational basis. We then prove that for classical bit sequences, Martin-Löf randomness agrees with its quantum analog under this embedding. Even in the classical setting our notion is broader, because probability measures over infinite bit, sequences can be viewed as states according to Remark 2.4. For instance, the uniform measure on $2^\mathbb{N}$, seen as the tracial state τ, is quantum ML-random. So in the new setting, randomness of ρ does not contradict that the function $n \to \rho \upharpoonright_n$ is computable. Philosophically there is some doubt whether these states should be called random at all; the term "unstructured" appears more apt, and only for classical bit sequences being unstructured actually implies being random. However, we prefer the term "random" here simply for practical reasons.

A. Quantum analog of Martin-Löf tests

Quite generally, a *projection* in a C^* algebra is a self-adjoint positive operator p such that $p^2 = p$. In the definition of ML-tests, we will replace a clopen set given by strings of length n by a projection in M_{2^n}. However, we need to restrict its possible matrix entries to complex numbers that have a finite description.

Definition 3.1. A complex number z is called *algebraic* if it is the root of a polynomial with rational coefficients. Let $\mathbb{C}_{\texttt{alg}}$ denote the field of algebraic complex numbers. A matrix over $\mathbb{C}_{\texttt{alg}}$ will be called *elementary*.

Clearly, such numbers are given by a finite amount of information, and in fact, they are polynomial time computable: for each n, one can in time polynomial in n compute a Gaussian rational within 2^{-n} of z. Note that if the matrix determining an operator on $\mathcal{H}_n$ consists of algebraic complex numbers, then its eigenvalues are in $\mathbb{C}_{\texttt{alg}}$ and its eigenvectors are vectors over $\mathbb{C}_{\texttt{alg}}$. We note that by a result of Rabin, $\mathbb{C}_{\texttt{alg}}$ has a computable presentation: there is a 1-1 function $f: \mathbb{C}_{\texttt{alg}} \to \mathbb{N}$ such that the image under f of the field operations are partial computable functions with computable domains.

Suppose that a projection $p \in M_{2^n}$ is diagonal with respect to the standard basis. Since its only possible eigenvalues are 0, 1, the entries are 0 or 1. Thus, projections in M_n with a diagonal matrix directly correspond to clopen sets in Cantor space.

For $u, v \in M_{2^n}$, one writes $u \leq v$ if $v - u$ is positive. Note that $p \leq q$ for projections $p, q \in M_{2^n}$ means that the range of p is contained in the range of q. A projection $p \in M_n$ with matrix entries in $\mathbb{C}_{\texttt{alg}}$ will be called a *special projection*. Such a projection has a finite description, given by the size of its matrix and all the entries in its matrix.

Definition 3.2. A quantum Σ_1^0 set (or q-Σ_1^0 set for short) G is a computable sequence of special projections $(p_i)_{i \in \mathbb{N}}$ such that $p_i \in M_{2^i}$ and $p_i \leq p_{i+1}$ for each i.

We note that the limit of an increasing sequence of projections $\langle p_i \rangle_{i \in \mathbb{N}}$ does not necessarily exist in M_{2^∞}. Such a limit would be a projection itself, and the projection lattice of M_{2^∞} is not complete. See, e.g., Ref. 11 where it is shown that its completeness would yield an embedding of the nonseparable C^*-algebra $\ell^\infty(\mathbb{C})$ into M_{2^∞}, which is not possible as the latter is separable.

Recall that for a state ρ and $p \in M_{2^n}$, we have $\rho(p) = \mathrm{Tr}(\rho \upharpoonright_n p)$ by (1). We write $\rho(G) = \sup_i \rho(p_i)$. In particular, we let $\tau(G) = \sup_i \tau(p_i)$, where τ is the tracial state defined in Sec. II F. Note that $\tau(G)$ is a real in [0, 1] that is the supremum of a computable sequence of rationals. Each Σ_1^0 set $\mathcal{S}$ in Cantor space is an effective union of clopen sets and hence can be seen as a q-Σ_1^0 set. If the state ρ is a measure, then $\rho(\mathcal{S})$ yields the usual result, evaluating ρ on $\mathcal{S}$.

We chose the term "quantum Σ_1^0 set" by analogy with the notion of Σ_1^0 subsets of Cantor space; they are not actually sets. The physical intuition is that a projection $p_i \in M_{2^i}$ describes a measurement of $\rho \upharpoonright_{M_{2^i}}$, strictly speaking given by the pair of projections $(p_i, I_{M_{2^i}} - p_i)$. Then, $\rho(p_i) = \mathrm{Tr}(\rho \upharpoonright_{M_{2^i}} p_i)$ is the outcome of the measurement, the probability that the first alternative given by the measurement occurs, and $\rho(G)$ is the overall outcome of measuring the state. So one could view G as a probabilistic set of states: for $0 \le \delta \le 1$, ρ is in G with probability δ if $\rho(G) > \delta$. The "inclusion relation" is $G \le H$ if $\rho(G) \le \rho(H)$ for each state ρ. We note that a "level set" of states $\{\rho : \rho(G) > \delta\}$ is open in $\mathcal{S}(M_{2^\infty})$ with the weak $*$ topology (Sec. II G).

For special projections $p, q \in M_{2^k}$, we denote by $p \vee q$ the projection in M_k with range $\mathtt{rg}\, p + \mathtt{rg}\, q$. We have $\tau(p \vee q) \le \tau(p) + \tau(q)$. For quantum Σ_1^0 sets $G = \langle p_k \rangle_{k \in \mathbb{N}}$ and $H = \langle q_k \rangle_{k \in \mathbb{N}}$, we define $G \vee H$ to be $\langle p_k \vee q_k \rangle_{k \in \mathbb{N}}$. Note that again $\tau(G \vee H) \le \tau(G) + \tau(H)$. Inductively, we then define $G_1 \vee \ldots \vee G_r$ for $r \ge 2$.

Definition 3.3 (Quantum Martin-Löf randomness). A *quantum Martin-Löf test* (qML-test) is an effective sequence $\langle G_r \rangle_{r \in \mathbb{N}}$ of quantum Σ_1^0 sets such that $\tau(G_r) \le 2^{-r}$ for each r. For $\delta \in (0, 1)$, we say that ρ *fails* the qML test *at order* δ if $\rho(G_r) > \delta$ for each r; otherwise, ρ *passes* the qML test *at order* δ. We say that ρ is *quantum ML-random* if it passes each qML test $\langle G_r \rangle_{r \in \mathbb{N}}$ at each positive order, that is, $\inf_r \rho(G_r) = 0$.

Proposition 3.4. There is a qML-test $\langle R_n \rangle$ such that for each qML test $\langle G_k \rangle$ and each state ρ, and for each n, there is k such that $\rho(R_n) \ge \rho(G_k)$. In particular, the test is universal in the sense that ρ is qML random iff ρ passes this single test.

Proof. This follows the usual construction due to Martin-Löf; see, e.g., Ref. 25, 3.2.4. We may fix an effective listing $\langle G_m^e \rangle_{m \in \mathbb{N}}$ ($e \in \mathbb{N}$) of all the quantum ML tests, where $G_m^e = \langle p_{m,r}^e \rangle_{r \in \mathbb{N}}$ for projections $p_{m,r}^e$ in M_{2^r}. Informally, we let

$$R_n = \bigvee_e G_{e+n+1}^e.$$

However, this infinite supremum of quantum Σ_1^0 sets is actually not defined. To interpret it, think of $\bigvee_e G_{e+n+1}^e$ as $\bigvee_e \bigvee_r p_{e+n+1,r}^e$ (which is still not defined). Now let

$$q_k^n = \bigvee_{e+n+1 \le k} p_{e+n+1,k}^e,$$

which is a finite supremum of projections. Clearly, $q_k^n \le q_{k+1}^n$, and $\tau(q_k^n) \le \sum_e \tau(p_{e+n+1,k}^e) \le 2^{-n}$. We let $R_n = \langle q_k^n \rangle_{k \in \mathbb{N}}$ so that $\tau(R_n) \le 2^{-n}$. Hence, $\langle R_n \rangle_{n \in \mathbb{N}}$ is a quantum ML-test.

Fix e. For each n, we have

$$\rho(R_n) = \sup_k \rho(q_k^n) \ge \sup_k \rho(p_{n+e+1,k}^e)$$

$$= \rho(G_{n+e+1}^e).$$

$\square$

A basic property one expects of random bit sequences Z is the law of large numbers, namely, $\lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} Z(i) = 1/2$. This property holds for Martin-Löf (or even Schnorr) random bit sequences; see, e.g., Ref. 25, 3.5.21. The first author and Tomamichel have proved a version of the law of large numbers for qML-random states. For $i < n$, let $S_{n,i}$ be the subspace of $\mathbb{C}^{2^n}$ generated by those $\underline{\sigma}$ with $\sigma_i = 1$. It is as usual identified with its orthogonal projection. So for any state ρ on M_{2^∞}, the real $\rho(S_{n,i}) = \mathrm{Tr}(\rho \upharpoonright_n S_i^n)$ is the probability that a measurement of the ith qubit of its initial segment $\rho \upharpoonright_n$ returns 1.

Proposition 3.5 (Ref. 10, Sec. 6.6). Let ρ be a qML-random state. We have

$$\lim_n \frac{1}{n} \sum_{i < n} \rho(S_{n,i}) = 1/2.$$

Their argument is based on Chernoff bounds. It works in more generality for any computable bias r in place of $1/2$ and for states that are qML-random with respect to that bias, as detailed in Ref. 10, Sec. 6.6.

B. Comparison with ML-randomness for bit sequences

Recall from Subsection II G that each bit sequence Z can be viewed as a state on M_{2^∞}. In this section, we show that Z if ML-random iff Z viewed as a state is qML-random (Theorem 3.9). Each classical ML-test can be viewed as quantum ML-test, so quantum ML-randomness implies ML-randomness for Z. For the converse implication, the idea is to turn a quantum ML-test that Z fails at order δ into a classical test that Z fails. We need a few preliminaries. We thank the anonymous referees for suggesting simplifications implemented in the argument below.

Recall that the vectors $\underline{\sigma}$, for n-bit strings σ, form the standard basis of $\mathcal{H}_n$. Note that if $p \in M_{2^k}$ is a projection and η is a bitstring of length k, then $\mathsf{Tr}(|\underline{\eta}\rangle\langle\underline{\eta}|p) = \|p(\eta)\|^2 = \langle\eta|p|\eta\rangle$. Given a bit sequence Z, letting $\eta = Z\!\upharpoonright_k$, we have $Z(p) = \mathsf{Tr}(|\underline{\eta}\rangle\langle\underline{\eta}|p)$ (if Z is viewed as a state, then $Z\!\upharpoonright_k$ is viewed as the density matrix $|\underline{\eta}\rangle\langle\underline{\eta}|$ in Dirac notation).

Definition 3.6. Fix $k \in \mathbb{N}$, and let $p \in M_{2^k}$ be a projection. For $\delta > 0$, define

$$S = S_{p,\delta}^k = \{\eta \in \{0,1\}^k \colon \delta \le \mathsf{Tr}(|\underline{\eta}\rangle\langle\underline{\eta}|p)\}. \tag{4}$$

In the following, we identify the set S of strings of length k in (4) with the corresponding diagonal projection in M_{2^k}. By $|S|$, we denote the size of the set S.

Claim 3.7. $\tau(S) \le \tau(p)/\delta$.

Proof. $\delta|S| \le \sum_{\eta \in S} \mathsf{Tr}(|\underline{\eta}\rangle\langle\underline{\eta}|p) \le \sum_\eta \mathsf{Tr}(|\underline{\eta}\rangle\langle\underline{\eta}|p) = \mathsf{Tr}(p)$, so $|S|2^{-k} \le \mathsf{Tr}(p)2^{-k}/\delta = \tau(q)/\delta$. $\square$

Claim 3.8. Suppose $p \in M_{2^k}$ are as above. Then,

$$S_{p',\delta}^{k+1} = \{\eta a \colon |\eta| = k, a = 0, 1 \ \wedge \ \eta \in S_{p,\delta}^k\},$$

where p' is the lifting of p to $M_{2^{k+1}}$.

Proof. For η, a as above, we have $p'(\underline{\eta a}) = p(\underline{\eta}) \otimes \underline{a}$ and so $\mathsf{Tr}(|\underline{\eta}\rangle\langle\underline{\eta}|p) = \|p(\eta)\|^2 = \|p'(\underline{\eta a})\|^2 = \mathsf{Tr}(|\underline{\eta a}\rangle\langle\underline{\eta a}|p')$. $\square$

Theorem 3.9. *Suppose $Z \in 2^{\mathbb{N}}$. Then, Z is ML-random iff Z viewed as an element of $\mathcal{S}(M_{2^\infty})$ is qML-random.*

Proof. Suppose Z fails the qML-test $\langle G^r\rangle_{r\in\mathbb{N}}$ at order $\delta > 0$, where G^r is given by the sequence $\langle p_k^r\rangle_{k\in\mathbb{N}}$. Thus, $\forall r \exists k\, Z(p_k^r) > \delta$, and $\sup_k \tau(p_k^r) \le 2^{-r}$. Uniformly in r, we will define a Σ_1^0 set $V_r \subseteq 2^{\mathbb{N}}$ containing Z and of measure at most $2^{-r}/\delta$. This will show that Z is not ML-random.

We fix r and suppress it from the notation for now. We may assume that $p_k \in M_{2^k}$ for each k. Define $S_{p_k,\delta}^k$ as in (4). We let $V^r = V = \bigcup_k \mathcal{S}_k$, where $\mathcal{S}_k = [S_{p_k,\delta}^k]^{\prec}$ (here, $[X]^{\prec}$ denotes the open set given by a set X of strings).

Clearly, $Z \in V$. It remains to verify that the uniform measure of V is at most $2^{-r}/\delta$. By Claim 3.7, it suffices to show that $\mathcal{S}_k \subseteq \mathcal{S}_{k+1}$ for each k. By Claim 3.8 viewing $p_k \in M_{2^{k+1}}$, we can evaluate (4) for $k + 1$ and obtain a set of strings generating the same clopen set $\mathcal{S}_k$. Since $p_k \le p_{k+1}$, this set of strings is contained in $S_{p_{k+1},\delta}^{k+1}$. $\square$

The first author and Stephan have studied the case of states that can be seen as measures on Cantor space in a separate paper.[26] They call a measure ρ Martin-Löf absolutely continuous if $\lim_m \rho(G_m) = 0$ for each ML-test $\langle G_m\rangle$. Tejas Bhojraj, a PhD student of Joseph Miller at UW Madison, has shown that this notion coincides with quantum ML-randomness for measures, generalizing the result above.

C. Solovay tests in the quantum setting

We discuss some quantum analogs of Solovay tests, a test notion that is equivalent to ML-tests in the classical setting (Ref. 25, Chap. 3). Quantum Solovay tests will be used in the statement of Theorem 4.4.

Definition 3.10 (Quantum Solovay randomness).

- A *quantum Solovay test* is an effective sequence $\langle G_r\rangle_{r\in\mathbb{N}}$ of quantum Σ_1^0 sets such that $\sum_r \tau(G_r) < \infty$.
- We say that the test is *strong* if G_r are given as projections; that is, from r, we can compute n_r and a matrix of algebraic numbers in $M_{2^{n_r}}$ describing $G_r = p_r$.
- For $\delta \in (0, 1)$, we say that ρ *fails* the quantum Solovay test *at order δ* if $\rho(G_r) > \delta$ for infinitely many r; otherwise, ρ *passes* the qML test *at order δ*.
- We say that ρ is *quantum Solovay-random* if it passes each quantum Solovay test $\langle G_r\rangle_{r\in\mathbb{N}}$ at each positive order, that is, $\lim_r \rho(G_r) = 0$.

Tejas Bhojraj has shown that quantum Martin-Löf randomness implies quantum Solovay randomness; the converse implication is trivial. He converts a quantum Solovay test into a quantum Martin-Löf test so that failing the former at level δ implies failing the latter at level $O(\delta^2)$.

IV. INITIAL SEGMENT COMPLEXITY

Our definition of quantum Martin-Löf randomness is by analogy with classical ML-randomness but also based on the intuition that the properties of quantum Martin-Löf random states are hard to predict. So we expect that the complexity of their initial segments is high. In order to formalize this, we start off from a theorem of Gács and also Miller and Yu[18] that asserts that a sequence Z is ML-random iff all its initial segments are hard to compress, in the sense of plain descriptive string complexity. Our main result works toward an extension of this theorem to the quantum setting.

A. Classical setting

Let $K(x)$ denote the prefix-free version of descriptive complexity of a bit string x. (See Ref. 25, Chap. 2 for a brief overview of descriptive string complexity, also called Kolmogorov complexity.) The Levin-Schnorr theorem (see Ref. 9, Theorem 5.2.3 or Ref. 25, Theorem 3.2.9) says that a bit sequence Z is ML-random if and only if each of its initial segments is incompressible in the sense that $\exists b \in \mathbb{N} \, \forall n \, K(Z \restriction_n) > n - b$. The Miller-Yu Theorem (Ref. 18, Theorem 7.1) is a version of this in terms of plain, rather than prefix-free, descriptive string complexity, usually denoted by $C(x)$. The constant b is replaced by a sufficiently fast growing computable function $f(n)$. We will provide a quantum analog of the Miller-Yu theorem, thereby avoiding the obstacles to introducing prefix-free descriptive string complexity in the quantum setting.

A slight variant of the Miller-Yu Theorem was obtained by Bienvenu, Merkle, and Shen.[5] Their version states that, for an appropriate computable function f such that $\sum 2^{-f(n)} < \infty$, Z is ML-random iff there is r such that for each n, we have $C(Z \restriction_n | n) \geq n - f(n) - r$, where $C(x|n)$ is the plain Kolmogorov complexity of a string x given its length n. Requiring $\sum_n 2^{-f(n)} < \infty$ of course means that f grows sufficiently fast; the borderline is between $\log_2 n$ and $2 \log_2 n$.

B. Quantum setting

Quantum Kolmogorov complexity is measured via quantum Turing machines.[3,30] In the version due to Berthiaume, van Dam, and Laplante (Ref. 4, Definition 7), the compression of a state of M_{2^n} is via a state of M_{2^k}, and only approximative in the sense that a state in M_{2^n} "nearby" the given state can actually be compressed. More detail on this was provided in Markus Müller's thesis,[22] which, in particular, contains a detailed discussion of how to define halting for a quantum Turing machine.

In order to avoid obscuring the arguments below by discussions of quantum Turing machines and universality, we will use a restricted machine model that is sufficient for a meaningful analog of the Gács-Miller-Yu Theorem. This machine model corresponds to uniformly generated circuit sequences. After proving our result, in Remark 4.7, we will discuss its relationship with quantum Kolmogorov complexity in the sense of Ref. 4.

Convention 4.1. In the following, all qubit sequences and all states will be elementary. Thus, the relevant matrices only have entries from the field $\mathbb{C}_{\text{alg}}$ of algebraic complex numbers.

Definition 4.2. A *unitary machine* L is given by computable sequence of unitary (elementary) matrices $L_n \in M_{2^n}$. For an input z which is a density matrix in M_{2^n}, its output is $L(z; n) := L_n z L_n^\dagger$. Thus, if z is a pure state $|\psi\rangle$, with the usual identifications the output is $L_n |\psi\rangle$.

Recall that the trace norm of an $n \times n$ matrix A over $\mathbb{C}$ is defined by $\|A\|_{\text{tr}} = \sqrt{\text{Tr}(AA^\dagger)}$. The trace distance between two $n \times n$ matrices is $D(A, B) = \frac{1}{2}\|A - B\|_{tr}$.

Definition 4.3. Let L be a unitary machine. The L-quantum Kolmogorov complexity $QC_L^\epsilon(x \mid n)$ of a (possibly mixed) state x on n-qubits is the least natural number k such that there exists a (mixed) state $y \in M_{2^k}$ with

$$D(x, L(y \otimes |0^{n-k}\rangle\langle 0^{n-k}|; n)) < \epsilon.$$

That is, the output of L on $y \otimes |0^{n-k}\rangle\langle 0^{n-k}|$ approximates x to an accuracy of ϵ in the trace distance.

We fix a computable listing $\langle \sigma_i \rangle_{i \in \mathbb{N}}$ of the elementary pure qubit strings so that $\ell(\sigma_i) \leq i$ for each i.
We now prove a weak quantum analog of the Gács-Miller-Yu theorem.

Theorem 4.4. Let ρ be a state on M_{2^∞}.

(1) Let L be a unitary machine. Let $1 > \varepsilon > 0$ and suppose ρ passes each qML-test at order $1 - \varepsilon$. Then for each computable function f satisfying $\sum_n 2^{-f(n)} < \infty$, for almost every n,

$$QC_L^\varepsilon(\rho \upharpoonright_n | n) \geq n - f(n).$$

(2) For each strong quantum Solovay test $\langle p_r \rangle_{r \in \mathbb{N}}$, there exists a total computable function $f \colon \mathbb{N} \to \mathbb{N}$ with $\sum_n 2^{-f(n)} \leq 4$ and a unitary machine L such that the following holds. If ρ fails $\langle p_r \rangle$ at order $1 - \varepsilon$ where $1 > \varepsilon > 0$, then there are infinitely many n such that

$$QC_L^{\sqrt{\varepsilon}}(\rho \upharpoonright_n | n) < n - f(n).$$

Note that this is not a full analog because the second part can only be obtained under the hypothesis that ρ fails a strong Solovay test (Definition 3.10). Bhojraj has announced an alternative version of Part 1 where the hypothesis is that ρ pass all strong Solovay tests at order $1 - \varepsilon$.

Proof. *Part 1*: We may assume that $\sum_n 2^{-f(n)} \leq 1/4$ because we can replace f by $\widetilde{f} = f + C$, where C is sufficiently large so that this condition is met.

Recall our fixed listing $\langle \sigma_i \rangle_{i \in \mathbb{N}}$ of the pure elementary quantum states of any length. For a given parameter $r \in \mathbb{N}$ and $t, n \in \mathbb{N}$, let $S_{r,t}(n)$ be the set of pure qubit strings $x = \sigma_i$, $i \leq t$, of length n so that for some pure qubit string $y = \sigma_k$, $k \leq t$, we have

$$|y| \leq n - f(n) - r \quad \text{and} \quad L(y \otimes |0^{n-|y|}\rangle; n) = x.$$

Note that $S_{r,t}(n)$ is computable in r, t, n using Convention 4.1. Hence, from r, t, n, we can compute an orthogonal projection $p_{r,t}(n)$ in M_{2^n} onto the subspace generated by $S_{r,t}(n)$. Let $p_{r,t} = \sup_{n \leq t} p_{r,t}(n)$. Then, $p_{r,t} \in M_{2^t}$ and $p_{r,t}$ is computable in r, t. Clearly, $p_{r,t} \leq p_{r,t+1}$ for each t.

By definition of unitary machines, the dimension of the range of $p_{r,t}(n)$ is bounded by $2^{n-f(n)-r+2}$. Hence, $\tau(p_{r,t}(n)) \leq 2^{-f(n)-r+2}$, and then $\tau(p_{r,t}) \leq \sum_n 2^{-f(n)-r+2} \leq 2^{-r}$ by our hypothesis on f.

Let G_r be the quantum Σ_1^0 set given by the sequence $\langle p_{r,t} \rangle_{t \in \mathbb{N}}$. Then, $\langle G_r \rangle_{r \in \mathbb{N}}$ is a quantum ML-test.

We show that there is r such that for each n, we have $QC_L^\varepsilon(\rho \upharpoonright_n | n) \geq n - f(n) - r$. Since we can carry out the same argument with $\lfloor \frac{1}{2} f \rfloor$ instead of f and $f(n) \to \infty$, this will be sufficient.

We proceed by contraposition. Suppose that for arbitrary $r \in \mathbb{N}$, there is n such that $QC_L^\varepsilon(\rho \upharpoonright_n | n) < n - f(n) - r$. This means that there is a state y (possibly mixed) of length $k < n - f(n) - r$ such that $D(x, \rho \upharpoonright_n) < \varepsilon$, where $x = L(y \otimes |0^{n-k}\rangle\langle 0^{n-k}|, n)$. Let $y = \sum \alpha_i |y_i\rangle\langle y_i|$ be the corresponding convex combination of pure states with α_i algebraic and y_i of length k. We have $x = \sum_i \alpha_i |x_i\rangle\langle x_i|$, where $x_i = L(y_i \otimes |0^{n-k}\rangle, n)$. Then, there is t such that $x_i \in S_{r,t}(n)$ for each i, and hence $\mathrm{Tr}[x p_{r,t}(n)] = 1$. This implies that $\rho(p_{r,t}(n)) > 1 - \varepsilon$ and hence $\rho(G_r) > 1 - \varepsilon$. Since r was arbitrary, this shows that ρ fails the test at order $1 - \varepsilon$.

Part 2: Let $\langle p_r \rangle_{r \in \mathbb{N}}$ be a strong quantum Solovay test. We may assume that $\sum_r \tau(p_r) \leq 1/2$ and that $p_r \in M_{2^{n_r}}$, where n_r is computed from r and $n_r < n_{r+1}$ for each r. The idea is as follows: suppose the range of p_r has dimension $k < n_r$. Then, z_n', the projection of $\rho \upharpoonright_n$ to p_r as defined below, can be directly described by a density matrix in M_{2^k} if we define our unitary machine L to compute an isometry between $\mathcal{H}_k$ and the range of p_r. If $\rho(p_r) > 1 - \varepsilon$, we show that the trace distance from z_n' to $\rho \upharpoonright_n$ is at most $\sqrt{\varepsilon}$. Therefore, $QC_L^{\sqrt{\varepsilon}}(\rho \upharpoonright_n | n) \leq k$. For a function f as required, we can ensure $k < n - f(n_r)$ for each r. For the details, let $f \colon \mathbb{N} \to \mathbb{N}$ be a computable function such that

$$2^{-f(n_r)} \geq \tau(p_r) > 2^{-f(n_r)-1}$$

and $f(m) = m$ if m is not of the form n_r. Note that f is computable and satisfies $\sum_n 2^{-f(n)} \leq 4$. Let $g(n) = n - f(n)$.

To describe the unitary machine L, we need to provide a computable sequence of unitary matrices $\langle L_n \rangle_{n \in \mathbb{N}}$. For $n = n_r$, let L_n be a unitary matrix in M_{2^n} such that its restriction $L_n \upharpoonright \mathcal{H}_{g(n)}$ is an isometry $\mathcal{H}_{g(n)} \cong \mathrm{rg}(p_r)$ (the range of p_r). By hypothesis on the sequence $\langle p_r \rangle$, this sequence of unitary matrices is computable.

For a projection operator p in M_{2^n} and a density matrix s in M_{2^n}, we define the projection of s by p to be

$$\mathrm{Proj}(s; p) = \frac{1}{\mathrm{Tr}[sp]} psp.$$

Note that this is again a density matrix, and each of its eigenvectors is in the range of p.

In the following, fix r such that $\rho(p_r) > 1 - \varepsilon$. Write $n = n_r$ and $z_n = \rho \upharpoonright_n \in M_{2^n}$. So $\mathrm{Tr}(z_n p_r) > 1 - \varepsilon$. Let

$$z_n' = \mathrm{Proj}(z_n; p_r).$$

Claim 4.5. $QC_L^\delta(z_n' \mid n) \leq g(n)$ *for each* $\delta > 0$.

Proof. Each eigenvector of z_n' is in the range of p_r. So there is a density matrix $y \in M_{2^{g(n)}}$ such that $L_n(y \otimes |0^{\otimes f(n)}\rangle\langle 0^{\otimes f(n)}|)L_n^\dagger = z_n'$. $\square$

We now argue that $D(z'_n, z_n) < \sqrt{\varepsilon}$ (recall that D denotes the trace distance). We rely on the following.

Proposition 4.6. Let p be a projection in M_{2^n}, and let θ be a density matrix in M_{2^n}. Write $\alpha = \mathtt{Tr}[\theta p]$. Let $\theta' = \text{Proj}(\theta; p)$. Then, $D(\theta', \theta) \leq \sqrt{1 - \alpha}$.

Proof. Let $|\psi_\theta\rangle$ be a purification of θ. Then, $\alpha^{-\frac{1}{2}} p |\psi_\theta\rangle$ is a purification of θ'. Uhlmann's theorem (e.g., Ref. 24, Theorem 9.4) implies

$$F(\theta', \theta) \geq \alpha^{-\frac{1}{2}} \langle \psi_\theta | p | \psi_\theta \rangle = \alpha^{\frac{1}{2}},$$

where $F(\sigma, \tau) = \mathtt{Tr}\sqrt{\sqrt{\sigma}\tau\sqrt{\sigma}}$ denotes fidelity. Now it suffices to recall from, e.g., Ref. 24, Eq. (9.110) that $D(\theta', \theta) \leq \sqrt{1 - F(\theta', \theta)^2}$. □

We apply Proposition 4.6 to $p = p_r$ and $\theta = z_n$ and $\theta' = z'_n$, where as above $n = n_r$. By hypothesis, $\alpha = \mathtt{Tr}[z_n p_r] = \rho(p_r) > 1 - \varepsilon$ and hence $\sqrt{1 - \alpha} < \sqrt{\varepsilon}$. Claim 4.5 now shows $QC_L^\varepsilon(z_n) \leq g(n)$.

Since there are infinitely many r such that $\rho(p_r) > 1 - \varepsilon$, we obtain Part 2 of Theorem 4.4. □

Remark 4.7. In an important extended abstract, Yao[32] proved that the quantum Turing machines (QTM) of Bernstein and Vazirani[3] can be simulated by quantum circuits with only a polynomial overhead in time. For recent work on such a simulation, see Ref. 19.

Yao also announced the converse direction: a QTM can simulate the input/output behavior of a computable sequence of quantum circuits. The argument is briefly discussed after the statement of Theorem 3 in Ref. 32 (also see Ref. 31). So with suitable input/output conventions, Definition 4.3 can be seen as a special case of the definition of QC_M^ε for a quantum Turing machine M as in Ref. 4, Definition 7.

We ignore at present whether Part 1 can be strengthened to general quantum Turing machines. The input/output behavior of such a machine is merely given by a quantum operation, for instance, because at the end of a computation the state has to be discarded.

On the other hand, since a QTM M can simulate the effect of the sequence of quantum circuits $\langle L_n \rangle$, and a universal QTM in the sense of Ref. 3 can simulate M with a small loss in accuracy, we obtain the following.

Corollary 4.8. In the setting of Part 2 of the theorem, we have $QC^{2\sqrt{\varepsilon}}(\rho \restriction_n | n) < n - f(n)$ for infinitely many n.

It would be interesting to find a version of Theorem 4.4 in terms of Gács' version of quantum Kolmogorov complexity, which is based on semidensity matrices rather than machines.[13]

V. OUTLOOK

As mentioned, randomness via algorithmic tests has been related to effective dynamical systems in papers such as Refs. 23 and 15. For a promising connection with quantum information processing, recall that a spin chain can be seen as a quantum dynamical system with the shift operation,[6] in analogy with the classical case with the shift operation on $2^{\mathbb{N}}$ that deletes the first bit of a sequence. An interesting potential application of our randomness notion is to obtain an effective quantum version of the Shannon-McMillan-Breiman (SMB) theorem from the 1950s (see, e.g., Ref. 29). That result is important in the area of data compression because it determines the asymptotic compression rate of sequences of symbols emitted by an ergodic source.

Let A be a finite alphabet, and let P be an ergodic probability measure on $A^{\mathbb{N}}$. Let $h(P)$ denote the entropy of P. The classical theorem states that for almost every $Z \in A^{\mathbb{N}}$, we have

$$h(P) = -\lim_n \frac{1}{n} \log P[Z \restriction_n]; \tag{5}$$

informally, $h(P)$ can be obtained by looking at the asymptotic "empirical entropy" along a random sequence Z.

The Shannon-McMillan (SM) theorem is a slightly weaker, earlier version of the full SMB theorem based on the notion of convergence in probability. Breiman then phrased the Shannon-McMillan theorem as a property of almost every sequence in the sense of the given ergodic measure. Bjelaković *et al.*[6] provided a quantum version of the SM-theorem. Their setting is the one of bi-infinite spin chains, or more generally, d-dimensional lattices; it can be easily adapted to the present setting.

Algorithmic versions of the SMB theorem[14,15] show that Martin-Löf randomness of Z relative to the computable ergodic measure is sufficient for (5) to hold. The question then is whether in the quantum setting, quantum ML-randomness relative to a computable shift-invariant ergodic state is sufficient.

The von Neumann entropy of a density matrix S is defined by $H(S) = -\mathtt{Tr}(S \log S)$. For a state ψ on M_{2^∞}, we let $h(\psi) = \lim_n \frac{1}{n} H(\psi \restriction_{M_{2^n}})$. For background and notions not defined here, see Ref. 10, Sec. 6.

Conjecture 5.1 (with Tomamichel). Let ψ be an ergodic computable state on M_{2^∞}. Let ρ be a state that is quantum ML-random with respect to ψ. Then, $h(\psi) = -\lim_n \frac{1}{n}\mathtt{Tr}(\rho \restriction_{M_{2^n}} \log(\psi \restriction_{M_{2^n}}))$.

Note that this reduces to the classical theorem in case ψ is a probability measure and ρ a bit sequence because each matrix $\rho\restriction_{M_n}\log(\psi\restriction_{M_n})$ is diagonal with at most one nonzero entry. Tomamichel and the first author have verified the conjecture in case μ is an i.i.d. state; see Ref. 10, Sec. 6. The first author and Stephan (Ref. 26, Theorem 23) have proved the conjecture in case that ψ and ρ are measures on Cantor space and the empirical entropy $-\frac{1}{n}\log\psi[x]$, for x an n-bit string, is bounded above (this means that ψ is close to the uniform measure).

ACKNOWLEDGMENTS

REFERENCES

[1] J. Bausch, T. Cubitt, A. Lucia, D. Perez-Garcia, and M. Wolf, "Size-driven quantum phase transitions," Proc. Natl. Acad. Sci. U. S. A. **115**(1), 19–23 (2018).

[2] F. Benatti, S. Oskouei, and A. Deh Abad, "Gacs quantum algorithmic entropy in infinite dimensional Hilbert spaces," J. Math. Phys. **55**(8), 082205 (2014).

[3] E. Bernstein and U. Vazirani, "Quantum complexity theory," SIAM J. Comput. **26**(5), 1411–1473 (1997).

[4] A. Berthiaume, W. Van Dam, and S. Laplante, "Quantum Kolmogorov complexity," in *2000 Proceedings 15th Annual IEEE Conference on Computational Complexity* (IEEE, 2000), pp. 240–249.

[5] L. Bienvenu, W. Merkle, and A. Shen, "A simple proof of the Miller-Yu theorem," Fundam. Inf. **83**(1-2), 21–24 (2008).

[6] I. Bjelaković, T. Krüger, R. Siegmund-Schultze, and A. Szkoła, "The Shannon-McMillan theorem for ergodic quantum lattice systems," Invent. Math. **155**(1), 203–222 (2004).

[7] O. Bratteli and D. Robinson, *Operator Algebras and Quantum Statistical Mechanics: Volume 1: C*-and W*-Algebras. Symmetry groups. Decomposition of States* (Springer Science & Business Media, 2012), First edition 1979.

[8] T. Cubitt, D. Perez-Garcia, and M. Wolf, "Undecidability of the spectral gap," Nature **528**(7581), 207–211 (2015); e-print arXiv:1502.04573.

[9] R. Downey and D. Hirschfeldt, *Algorithmic Randomness and Complexity* (Springer-Verlag, Berlin, 2010).

[10] A. Nies (editor), "Logic blog 2017," e-print arXiv:1804.05331 (2017).

[11] R. Furber, Projections in CAR (canonical anticommutation relation) algebra, MathOverflow. URL: https://mathoverflow.net/q/334640, version: 2019-06-24.

[12] P. Gács, "Exact expressions for some randomness tests," Z. Math. Logik Grundlag. Math. **26**(5), 385–394 (1980).

[13] P. Gács, "Quantum algorithmic entropy," in *2001 16th Annual IEEE Conference on Computational Complexity* (IEEE, 2001), pp. 274–283.

[14] M. Hochman, "Upcrossing inequalities for stationary sequences and applications," Ann. Probab. **37**(6), 2135–2149 (2009).

[15] M. Hoyrup, "The dimension of ergodic random sequences," in *STACS*, edited by C. Dürr and T. Wilke (Springer, 2012), pp. 567–576.

[16] L. Levin, "Laws of information conservation (nongrowth) and aspects of the foundation of probability theory," Problemy Peredachi Informatsii **10**(3), 30–35 (1974).

[17] P. Martin-Löf, "The definition of random sequences," Inf. Control **9**, 602–619 (1966).

[18] J. Miller and L. Yu, "On initial segment complexity and degrees of randomness," Trans. Am. Math. Soc. **360**, 3193–3210 (2008).

[19] A. Molina and J. Watrous, "Revisiting the simulation of quantum turing machines by quantum circuits," Proc. R. Soc. A **475**(2226), 20180767 (2019).

[20] B. Monin and A. Nies, "A unifying approach to the Gamma question," in *Proceedings of Logic in Computer Science (LICS)* (IEEE Press, 2015).

[21] B. Monin and A. Nies, "Muchnik degrees and cardinal characteristics," preprint arXiv:1712.00864 (2017).

[22] M. Müller, "Quantum Kolmogorov complexity and the quantum Turing machine," Ph.D. thesis, University of Berlin, 2007; e-print arXiv:0712.4377.

[23] S. Nandakumar, "An effective ergodic theorem and some applications," in *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing* (ACM, 2008), pp. 39–44.

[24] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (AAPT, 2002).

[25] A. Nies, *Computability and Randomness*, Volume 51 of Oxford Logic Guides (Oxford University Press, Oxford, 2009), p. 444, paperback version 2011.

[26] A. Nies and F. Stephan, "A weak randomness notion for measures," e-print arXiv:1902.07871 (2019).

[27] N. Pathak, C. Rojas, and S. G. Simpson, "Schnorr randomness and the Lebesgue differentiation theorem," Proc. Am. Math. Soc. **142**(1), 335–349 (2014).

[28] C. P. Schnorr, "A unified approach to the definition of random sequences," Math. Syst. Theory **5**(3), 246–258 (1971).

[29] P. Shields, *The Ergodic Theory of Discrete Sample Paths*, Graduate Studies in Mathematics Vol. 13 (American Mathematical Society, 1996).

[30] U. Vazirani, "A survey of quantum complexity theory," in Proc. Symp. Appl. Math. **58**, 193–217 (2002).

[31] C. Westergaard, *Computational Equivalence between Quantum Turing Machines and Quantum Circuit Families* (University of Copenhagen, Denmark, 2005), available on Semantic Scholar.

[32] A. Yao, "Quantum circuit complexity," in *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science* (IEEE, 1993), pp. 352–361.