Algorithmic Randomness and Kolmogorov Complexity for Qubits

By

Tejas Bhojraj

A dissertation submitted in partial fulfillment of the

requirements for the degree of

Doctor of Philosophy

(Mathematics)

at the

UNIVERSITY OF WISCONSIN – MADISON

2021

Date of final oral examination: August 9, 2021

The dissertation is approved by the following members of the Final Oral Committee:

Joseph Miller, Professor, Mathematics, UW-Madison

André Nies, Professor, Computer Sciences, University of Auckland

Uri Andrews, Associate Professor, Mathematics, UW-Madison

Jin-Yi Cai, Professor, Computer Sciences, UW-Madison

Abstract

This work extends the theories of algorithmic randomness and Kolmogorov complexity of bitstrings to the quantum realm. Nies and Scholz defined quantum Martin-Löf randomness (q-MLR): the first notion of algorithmic randomness to be defined for infinite sequences of qubits, which are called *states*. We define a notion of quantum Solovay randomness and show it to be equivalent to q-MLR using purely linear algebraic methods. Quantum Schnorr randomness is then introduced. A quantum analogue of the law of large numbers is shown to hold for quantum Schnorr random states.

We next turn to a quantum analogue of Kolmogorov complexity. We introduce quantum-K (QK), a measure of the descriptive complexity of density matrices using classical prefix-free Turing machines and show that the initial segments of weak Solovay random and quantum Schnorr random states are incompressible in the sense of QK. Many properties enjoyed by prefix-free Kolmogorov complexity (K) have analogous versions for QK; notably a counting condition. Several connections between Solovay randomness and K, including the Chaitin type characterization of Solovay randomness, carry over to those between weak Solovay randomness and QK. Schnorr randomness has a Levin–Schnorr characterization using K_C; a version of K defined using an arbitrary computable measure machine, C. We similarly define QK_C, a version of QK. Quantum Schnorr randomness is shown to have a Levin–Schnorr and a Chaitin type characterization using QK_C.

We then show how classical randomness can be generated from a computable, non-quantum random state. We formalize how 'measurement' of a state induces a probability

measure on the space of infinite bitstrings. A state is 'measurement random' (mR) if the measure induced by it, under any computable basis, assigns probability one to the set of Martin-Löf randoms. I.e., measuring a mR state produces a Martin-Löf random bitstring with probability one. While quantum-Martin-Löf random states are mR, we show that the converse fails by defining a computable mR state ρ which is not quantum-Martin-Löf random. In fact, something stronger is true. Measuring ρ in any computable basis yields an arithmetically random sequence with probability one.

The work concludes by studying the asymptotic von Neumann entropy of computable states.

Acknowledgements

Joe Miller's warmth, approachability, sense of humor and willingness to discuss virtually anything under the sun made for an enjoyable and memorable time as his PhD student. I am indebted to him for his unfailing encouragement and for his open-mindedness in allowing me to choose for my thesis work, a topic which was initially unfamiliar not just to him but also to me (quantum information). I am grateful to André Nies for his advice and support. His paper [31] was responsible for introducing me to the theme dealt with in this thesis.

I thank Joe Miller, Steffen Lempp and Uri Andrews for fostering my interest in computability theory and logic during my undergraduate years. I thank my teachers (too many to name individually) at UW-Madison for imparting ideas and techniques which I am sure will have an enduring influence on my future work.

Contents

Chapter 1

Introduction

Quantum physics describes a physical system by a unit vector in an appropriate vector space. Although the vector space can be infinite dimensional in general, this thesis deals purely with finite dimensional spaces. The simplest setting is that of a two dimensional vector space: a qubit is a unit vector in $\mathbb{C}^2$ and describes a two dimensional quantum system. Consider the orthonormal basis of $\mathbb{C}^2$ comprised of the unit eigenvectors of the z-operator denoted (in the usual bra-ket notation) by $|0\rangle$ and $|1\rangle$. Recall that the z-operator is a Hermitian operator measuring the spin of a two dimensional quantum system in the z direction [27]. An arbitrary qubit has the form $\alpha|0\rangle + \beta|1\rangle$ where $|\alpha|^2 + |\beta|^2 = 1$. The $|0\rangle$ and $|1\rangle$ are the quantum analogues of the classical 0 and 1 respectively. While a bit can only take on two possible values (0 or 1), a qubit can be any unit length *linear combination* of the basis vectors $|0\rangle$ and $|1\rangle$. So, a qubit generalizes the classical bit. This suggests that notions concerning classical bits can be extrapolated to qubits.

Section 1.1, which may be skipped by the reader familiar with quantum theory, reviews some quantum theory background relevant to this work.

Information theory has been generalized to the quantum realm [27]. Similarly, the theory of computation has been extended to the quantum setting, a notable example being the conception of a quantum Turing machine [7, 26]. It hence seems natural to

extend algorithmic randomness, a discipline using concepts from computation and information, to the quantum realm. Algorithmic randomness studies the randomness of infinite bitstrings using two main tools: (1) effective measure theory and (2) Kolmogorov complexity. While classical Kolmogorov complexity has inspired many competing definitions of quantum Kolmogorov complexity [8, 26, 35], effective measure theory has only recently been extended to the quantum setting [11, 31].

What does algorithmic randomness study? Consider infinite sequences of ones and zeroes (called bitstrings in this paper). First consider the bitstring $101010101010\cdots$. It has an easily describable 'pattern' to it; namely that the ones and zeroes alternate. Now take a bitstring obtained by tossing a fair coin repeatedly. Intuitively, it seems that the second bitstring, in contrast to the first, is unlikely to have patterns. Algorithmic randomness tries to quantify our intuition that the second bitstring is more 'random', more 'structureless' than the first. For this, it uses two central concepts: (1) An effectively null set and (2) Kolmogorov complexity. Roughly speaking an 'effectively null set' is one which can be approximated by a computable sequence of open sets whose measures tend to zero in a nice way. Varying the precise definition of 'effectively null' yields various randomness notions such as for example, Martin-Löf randomness, Solovay randomness and Schnorr randomness. See [28] and [21] for more details on effective measure theory and its use in algorithmic randomness.

The Kolmogorov theoretical approach quantifies the randomness of infinite bitstrings by measuring the incompressibility of their finite initial segments. Roughly speaking, a finite bitstring σ is 'incompressible' if $K(\sigma)$ is close to $|\sigma|$. Here, K stands for the prefix-free Kolmogorov complexity. See [28] and [21] for an exposition on K and its properties. The Kolmogorov theoretical approach considers an infinite bitstring X to

be 'random' if its finite initial segments are asymptotically incompressible as n goes to infinity. I.e., if $X \upharpoonright n$ is the first n bits of X, then $K(X \upharpoonright n)$ is close to n as n tends to infinity.

It turns out that the randomness of an infinite bitstring measured via the effective measure theory approach is intimately related to its randomness measured in terms of their initial segment incompressibility.

While algorithmic randomness is concerned with the randomness of bitstrings, the present thesis is concerned with *quantum* algorithmic randomness: the study of the randomness of *qubitstrings* (infinite sequences of qubits), also called *states* [11, 31].

Building on the work of Nies and Scholz [31], Chapter 2 extends the classical effective measure theory approach to the quantum realm. It studies the quantum analogues of Martin-Löf, Solovay and Schnorr randomness, which are defined using effectively null sets in the classical theory. Chapter 3 extends the theory of classical Kolmogorov complexity to the quantum setting. It introduces quantum-K (QK), a quantum version of K, and relates it to the three quantum randomness notions defined in Chapter 2. The remaining two chapters explore interesting applications of the main theory developed in Chapters 2 and 3. In Chapter 4, we construct a computable state which is *not* quantum Martin-Löf random but which yields an arithmetically random bitstring with probability one when 'measured' (the notion of measuring a state is also defined in Chapter 4). Arithmetic randomness is a strong form of classical randomness, strictly stronger than Martin-Löf randomness (See 6.8.4 in [21] for details on arithmetic randomness).

The final chapter explores the von-Neumann entropies of the finite initial segments of computable states.

Section 1.1 reviews some background from quantum theory and the following sections

give an overview of each chapter.

1.1 Quantum theory background

A more detailed account may be found in the textbook by Nielsen and Chuang [27]. We assume the reader to be familiar with the bra-ket notation. A n-dimensional system is described by $|\psi\rangle$, a unit vector in $\mathbb{C}^n$. A physical quantity corresponds to a Hermitian operator H on $\mathbb{C}^n$. By Hermicity, H has a spectral decomposition:

$$H = \sum_{i \leqslant n} e_i |i\rangle\langle i|$$

where, $(|i\rangle)_{i \leqslant n}$ is the complete orthonormal set of eigenvectors of H. Measuring H on $|\psi\rangle$ produces outcome e_i with probabilty $|\langle i|\psi\rangle|^2 = Tr(|\psi\rangle\langle\psi||i\rangle\langle i|)$. So, the outcome is non-deterministic except when the $|\psi\rangle$ is an eigenvector of H. The only possible outcomes of measurement of H are its eigenvalues. If the outcome is e_i, the post-measurement system is in the eigenspace spanned by $\{|j\rangle : e_j = e_i\}$. In particular, if all the e_is are distinct, then the post-measurement system is $|i\rangle$ if the measurement outcome is e_i. As usual, we denote the eigenvectors of the z-operator (a operator on $\mathbb{C}^2$) by $|1\rangle$ and $|0\rangle$. Any $|\psi\rangle = \alpha|1\rangle + \beta|0\rangle$ with $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$ is said to be a *qubit*. A sequence of n qubits is modeled by a unit vector in $(\mathbb{C}^2)^{\otimes n}$ which has an orthonormal basis comprised of elements of the form

$$\bigotimes_{i<n} |\sigma(i)\rangle := |\sigma\rangle \text{ for a } \sigma \in \{0,1\}^n$$

States which are not pure tensors are said to be *entangled*. If $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ is entangled, its subsystem in $(\mathbb{C}^2)^{\otimes k}$ for some $k < n$ is not a single quantum state but rather is a probabilistic mixture of multiple quantum states. To describe such subsystems, we

reformulate the above in the density matrix language by replacing $(\mathbb{C}^2)^{\otimes n}$ with L_n, the space of linear operators on $(\mathbb{C}^2)^{\otimes n}$ and by replacing $|\psi\rangle$ with $|\psi\rangle\langle\psi|$. A positive semidefinite matrix $\rho \in L_n$ is a density matrix if $\mathrm{Tr}(\rho) = 1$. By Hermicity, ρ has a complete orthonormal set of eigenvectors $(\psi_i)_{i<2^n}$. So, it is unitarily diagonalizable and has eigenpairs (α_i, ψ_i)

$$\rho = \sum_{i<2^n} \alpha_i |\psi_i\rangle\langle\psi_i| \tag{1.1}$$

This sum must be convex as, $1{=}\mathrm{Tr}(\rho){=}\sum_i \alpha_i$. A density matrix $\rho \in L_n$ is said to be a *strictly mixed* state if 1.1 is a strictly convex sum and is said to be a *pure* state if $\rho = |\psi\rangle\langle\psi|$ for some unit vector ψ. A density matrix which may be pure or strictly mixed is simply referred to as a *mixed* state. In the density matrix language, a system $|\psi\rangle$ is represented by the pure state $|\psi\rangle\langle\psi|$. A system which is in $|\psi_i\rangle\langle\psi_i|$ with probability α_i is described by the mixed state $\rho = \sum_{i<2^n} \alpha_i |\psi_i\rangle\langle\psi_i|$. Measuring H on ρ produces outcome e_i with probabilty $|\langle i|\rho|i\rangle|^2 = Tr(\rho|i\rangle\langle i|)$. The expected value of measuring H on ρ is

$$[H]_\rho := \sum_i e_i Tr(\rho|i\rangle\langle i|) = Tr(H\rho)$$

A system which is a composite of systems given by $\sigma \in L_n$ and $\tau \in L_k$ is described by $\rho = \sigma \otimes \tau \in L_{n+k}$.

1.2 An Overview of Chapter Two

This chapter concerns the generalization of effective measure theory as used in classical algorithmic randomness to the quantum world. The basic definitions from algorithmic randomness we state below may be found in books by Nies [21] and Downey and

Hirschfeldt [28]. Roughly speaking, a Martin-Löf random bitstring is one which has no algorithmically describable regularities. Slightly more rigorously, an infinite bitstring is said to be Martin-Löf random if it is not in any 'effectively null' set. In the context of Martin-Löf randomness, a measurable set A is effectively null if there is a computable sequence of effective open sets, $(U_n)_n$ such that the measure of U_n is at most 2^{-n} and $A \subseteq U_n$ for all n. By varying the definition of 'effectively null', we get other notions of randomness like Solovay randomness and Schnorr randomness. Note that the randomness of a bitstring defined using this approach crucially depends on the notion of computability. In a broad sense, a bitstring is random if it has no '*computably describable*' patterns.

The notion of a computable real number will come up when we discuss quantum Schnorr randomness.

Definition 1.1. A real number r is said to be *computable* if there is a computable function f such that for all n, $|f(n) - r| < 2^{-n}$.

We describe how classical algorithmic randomness generalizes to qubitstrings. We refer the reader to the book by Nielsen and Chuang [27] for preliminaries on quantum theory.

While it is clear what one means by a infinite sequence of bits, it is not immediately obvious how one would formalize the notion of an infinite sequence of qubits. Many authors have independently come up with notions describing infinite sequences of qubits [6, 12, 31]. We will use the one given by Nies and Scholz [31] called a *state*. Recall that a positive semidefinite matrix with trace equal to one is called a 'density matrix' and is commonly used to represent a probabilistic mixture of pure quantum states (See [27]).

Definition 1.2 ([31]). A *state* $\rho = (\rho_n)_{n\in\mathbb{N}}$ is an infinite sequence of density matrices such that $\rho_n \in \mathbb{C}^{2^n\times 2^n}$ and $\forall n$, $PT_{\mathbb{C}^2}(\rho_n) = \rho_{n-1}$.

The idea is that ρ represents an infinite sequence of qubits whose first n qubits are given by ρ_n. Here, $PT_{\mathbb{C}^2}$ denotes the partial trace which 'traces out' the last qubit from $\mathbb{C}^{2^n}$. The definition requires ρ to be coherent in the sense that for all n, when ρ_n is 'restricted' via the partial trace to its first $n-1$ qubits, it has the same measurement statistics as the state on $n-1$ qubits given by ρ_{n-1}.

Definition 1.3 ([31]). Let $\tau = (\tau_n)_{n\in\mathbb{N}}$ be the state given by setting $\tau_n = \otimes_{i=1}^{n} I$ where I is the two by two identity matrix.

Definition 1.4 ([31]). A *special projection* is a hermitian projection matrix with complex algebraic entries.

Since the complex algebraic numbers (roots of polynomials with rational coefficients) have a computable presentation, we may identify a special projection with a natural number and hence talk about computable sequences of special projections. Let I denote the two by two identity matrix.

Definition 1.5 ([31]). A quantum Σ_1^0 set (or q-Σ_1^0 set for short) G is a computable sequence of special projections $G = (p_i)_{i\in\mathbb{N}}$ such that p_i is 2^i by 2^i and range$(p_i \otimes I) \subseteq$ range (p_{i+1}) for all $i \in \mathbb{N}$.

While a 2^n by 2^n special projection may be thought of as a computable projective measurement on a system of n qubits, a q-Σ_1^0 class corresponds to a computable sequence of projective measurements on longer and longer systems of qubits. We motivate the definition of a quantum Σ_1^0 set by relating it to the classical Σ_1^0 class. Let 2^ω, called

Cantor space, denote the collection of infinite bitstrings, let 2^n denote the set of bit strings of length n, $2^{<\omega} = \bigcup_n 2^n$, and let $2^{\leqslant\omega} := 2^{<\omega} \cup 2^\omega$. Cantor space can be topologized by declaring the cylinders to be the basic open sets. If $\pi \in 2^n$ for some n, then the cylinder generated by π, denoted $[\![\pi]\!]$, is the set of all sequences extending π:

$$[\![\pi]\!] = \{X \in 2^\omega : X \upharpoonright n = \pi\}.$$

If $C \subseteq 2^n$, let

$$[\![C]\!] := \bigcup_{\pi \in C} [\![\pi]\!],$$

be the set of all $X \in 2^\omega$ such that the initial segment of X of length n is in C. One of the many equivalent ways of defining a Σ^0_1 class is as follows.

Definition 1.6. A Σ^0_1 class $S \subseteq 2^\omega$ is any set of the form,

$$S = \bigcup_{i \in \mathbb{N}} [\![A_i]\!]$$

where

1. $A_i \subseteq 2^i, \forall i \in \mathbb{N}$
2. The indices of A_i form a computable sequence. (Being a finite set, each A_i has a natural number coding it.)
3. $[\![A_i]\!] \subseteq [\![A_{i+1}]\!], \forall i \in \mathbb{N}$.

Letting $[\![A_i]\!] := S_i$, we write $S = (S_i)_i$. A Σ^0_1 class S is coded (non-uniquely) by the index of the total computable function generating the sequence $(A_i)_{i \in \mathbb{N}}$ occurring in (2) in the definition of S. Hence, the notion of a computable sequence of Σ^0_1 classes makes sense. One sees that the special projections q_i in the definition of the q-Σ^0_1 play

the role of the A_i's which generate the Σ^0_1 class S. The following notion is a quantum analog of the Lebesgue measure of S, which equals $\lim_n(2^{-n}|A_n|)$, where $|.|$ refers to the cardinality. (The uniform measure on 2^ω is the measure induced by letting the measure of $[\![\tau]\!]$ be $2^{-|\tau|}$ for each $\tau \in 2^{<\omega}$. Here, $|\tau| := n$ if $\tau \in 2^n$.)

Definition 1.7 ([31])**.** If $G = (p_n)_{n\in\mathbb{N}}$ is a q-Σ^0_1 class, define $\tau(G) := \lim_n(2^{-n}|q_n|)$ where, $|q_n|$ is the rank of q_n.

Informally, and somewhat inaccurately, a q-Σ^0_1 class, $G = (p_n)_{n\in\mathbb{N}}$, may be thought of as a projective measurement whose expected value, when 'measured' on a state $\rho = (\rho_n)_{n\in\mathbb{N}}$ is $\rho(G) := \lim_n \text{Trace } (\rho_n p_n)$. In reality, a q-$\Sigma^0_1$ class, $G = (p_n)_n$, is a sequence of projective measurements on larger and larger finite dimensional complex Hilbert spaces. This sequence can be used to 'measure' a coherent sequence of density matrices (i.e., a state), the expected value of which is the limit of the Trace$(\rho_n p_n)$ (the expected value of measuring the n^{th} 'level').

Definition 1.8. A *classical Martin-Löf test* (MLT) is a computable sequence $(S_m)_{m\in\mathbb{N}}$ of Σ^0_1 classes such that the Lebesgue measure of S_m is less than or equal to 2^{-m} for all m.

Its quantum generalization is:

Definition 1.9 ([31])**.** A *quantum Martin-Löf test* (q-MLT) is a computable sequence, $(S_m)_{m\in\mathbb{N}}$ of q-Σ^0_1 classes such that $\tau(S_m)$ is less than or equal to 2^{-m} for all m.

Definition 1.10 ([31])**.** A state ρ is *q-MLR* if for any q-MLT $(S_m)_{m\in\mathbb{N}}$, $\inf_{m\in\mathbb{N}} \rho(S_m) = 0$.

Roughly speaking, a state is q-MLR if it cannot be 'detected by projective measurements of arbitrarily small rank'.

Definition 1.11 ([31])**.** A state ρ is said to *fail the q-MLT* $(S_m)_{m\in\mathbb{N}}$*, at order* δ, if $\inf_{m\in\mathbb{N}} \rho(S_m) > \delta$. ρ is said to *pass the q-MLT* $(S_m)_{m\in\mathbb{N}}$ *at order* δ if it does not fail it at δ.

So, ρ is q-MLR if it passes all q-MLTs at all $\delta > 0$.

Remark 1.12. A few remarks on notation: By 'bitstring', we mean a finite or infinite classical sequence of ones and zeroes. It will be clear from context whether the specific bitstring under discussion is finite or infinite. We use 2^n to denote the set of bitstrings of length n. Let B^n denote the standard computational basis for $\mathbb{C}^{2^n}$. I.e., $B^n := \{|\sigma\rangle : \sigma \in 2^n\}$. If $S \subseteq 2^n$, let $P_S := \sum_{\sigma\in S} |\sigma\rangle\langle\sigma|$. 'Tr' stands for trace. A sequence of q-Σ_1^0 classes will be indexed by the superscript. The subscript will index the sequence of special projections comprising a q-Σ_1^0. For example, $(S^m)_{m\in\mathbb{N}}$ is a sequence of q-Σ_1^0 classes and $S^m = (S_n^m)_{m\in\mathbb{N}}$ is a class from the sequence. So, a sequence of q-Σ_1^0 classes can be thought of as a double sequence of special projections: $(S_n^m)_{m,n\in\mathbb{N}}$. Lebesgue measure is denoted by μ.

In addition to continuing the investigation of quantum Martin-Löf randomness begun by Nies and Scholz [31], we introduce and study quantum Solovay and quantum Schnorr randomness in Chapter 2.

1.3 An Overview of Chapter Three

As mentioned before, effective measure theory (using 'effectively null sets') and Kolmogorov complexity theory (using descriptive complexity of initial segments) are two seemingly unrelated but equivalent approaches to study the randomness of bitstrings. Chapter 2 of this thesis and other works [9,11,31] have generalized the first approach to

the quantum realm. We work towards generalizing the second approach in Chapter 3 of which we give an overview here.

The most basic definition from the classical theory is that of K: The prefix-free Kolmorogov Complexity (K) of a finite bit string σ is defined as

$$K(\sigma) = \min\{|x| : \mathbb{U}(x) = \sigma\},$$

where the x's are finite bitstrings and $\mathbb{U}$ is the universal prefix-free Turing Machine (See [21,28] for detailed expositions). Martin-Löf randomness (which is equivalent to Solovay randomness) and Schnorr randomness for infinite bitstrings, defined using the concept of 'effective null sets', have characterizations in terms of prefix-free complexity [14, 21, 28]. The Chaitin characterization (See [16] and theorem 3.2.21 in [28]),

$$X \text{ is Martin-Löf random } \iff \lim_n K(X \upharpoonright n) - n = \infty,$$

and the Levin–Schnorr characterization (See theorem 3.2.9 in [28]),

$$X \text{ is Martin-Löf random } \iff \exists c \forall n [K(X \upharpoonright n) > n - c],$$

are important characterizations of Martin-Löf randoms. A prefix-free machine C is said to be a computable measure machine if the Lebesgue measure of its domain is a computable real number [20]. For an arbitrary computable measure machine C we define [20]

$$K_C(\sigma) = \min\{|x| : C(x) = \sigma\}.$$

Schnorr randomness has a Levin–Schnorr type characterization using K_C;

$$X \text{ is Schnorr random } \iff \forall C \exists c \forall n [K_C(X \upharpoonright n) > n - c].$$

Quantum Solovay randomness and quantum Schnorr randomness for states are defined in Chapter 2. Analogously to the classical situation, one may explore the connections between quantum Solovay randomness and quantum Schnorr randomness and the initial segment descriptive complexity of states.

Motivated by this, we asked whether there is a quantum analogue of K which yields a characterization of quantum Solovay and quantum Schnorr randomness. We define a family $(QK^\epsilon)_{\epsilon>0}$ of complexity measures for density matrices based on prefix-free, classical Turing machines. The abbreviation QK stands for 'quantum-K', reflecting our intention of developing a quantum analogue of K, the classical prefix-free Kolmogorov complexity.

To the best of our knowledge, all notions of quantum Kolmogorov complexity developed so far, with one exception [35], exclusively use machines which are not prefix-free (plain classical machines or quantum Turing machines) [7, 8, 26]. K_Q, a notion developed in [35] uses a quantum Turing machine, Q together with the classical prefix-free Kolmogorov complexity in its definition.

Many properties enjoyed by K, notably a counting condition, have analogous versions for QK^ϵ for each fixed $\epsilon > 0$. Many connections between Solovay randomness and K, including the Chaitin type characterization of Solovay randomness, carry over to those between weak Solovay randomness and QK^ϵ for each fixed $\epsilon > 0$. We work towards a Levin–Schnorr type characterization of weak Solovay randomness in terms of $(QK^\epsilon)_{\epsilon>0}$.

As mentioned above, Schnorr randomness has a Levin–Schnorr characterization using the family of complexity measures $\{K_C : \text{C is a computable measure machine}\}$. We similarly define the family $\{QK^\epsilon_C : \epsilon > 0, \text{ C is a computable measure machine}\}$. Each

QK^{ϵ}_{C} here is defined exactly like QK^{ϵ} with C replacing the universal prefix-free Turing machine. Quantum Schnorr randomness is shown to have a Levin–Schnorr and a Chaitin type characterization using the family $\{QK^{\epsilon}_{C} : \epsilon > 0, \text{ C is a computable measure machine}\}$. The latter implies a Chaitin type characterization of classical Schnorr randomness using $\{K_C : \text{C is a computable measure machine}\}$.

1.4 An Overview of Chapter Four

This chapter investigates the following question: Can the quantum non-randomness of a state always be detected using 'qubitbitwise measurements'? To make this question fully precise, we need to define what we mean by 'qubitbitwise measurements'. To this end, we formalize a notion of 'measuring a state'. With this notion in hand, we will construct a computable, non-q-MLR state which yields a MLR bitstring almost surely when measured qubitwise. This implies that it is not always possible to detect q-MLR using only qubitwise measurements.

Measuring a finite dimensional quantum system or a composite system of finitely many qubits is a pivotal concept in quantum information theory [17]. It hence seems natural to consider defining a notion of 'measuring' a state. We first formalize how 'measurement' of a state in a basis induces a probability measure on Cantor space. A state is 'measurement random' (mR) if the measure induced by it, under any computable basis, assigns probability one to the set of Martin-Löf randoms. Equivalently, a state is mR if and only if measuring it in any computable basis yields a Martin-Löf random with probability one. While quantum-Martin-Löf random states are mR, the converse fails: there is a mR state, ρ which is not quantum-Martin-Löf random. In fact, something

stronger is true. While ρ is computable and can be easily constructed, measuring it in any computable basis yields an arithmetically random sequence with probability one. I.e., classical arithmetic randomness can be generated from a computable, non-quantum random sequence of qubits.

1.5 An Overview of Chapter Five

As quantum Martin-Löf randomness is a notion of 'randomness' for states, we don't expect computable states to be quantum Martin-Löf random. However, the tracial state, which is computable, is quantum Martin-Löf random. This rather surprising fact justifies a study of the computable quantum Martin-Löf randoms. The theme of this chapter is to use the von Neumann entropy as a measure of the randomness of computable states.

Recall that the von-Neumann entropy of a density matrix is the Shannon entropy of the distribution given by its eigenvalues (As a density matrix is positive semidefinite and has trace equal to one, its eigenvalues are real non-negative and sum to one. The eigenvalues hence form a probability distribution. See, for example [27]). So, the von-Neumann entropy of a density matrix d reflects how 'evenly spread out' its eigenvalues are. If the eigenmass of d is 'concentrated' at a few (relative to the dimension of d) eigenvectors then the von Neumann entropy of d is low. Informally speaking, if a computable density matrix d has a low entropy, then the few eigenvectors at which the eigenmass is concentrated can be used to construct a special projection 'close' to d. Conversely, if the von Neumann entropy of d is high, then one cannot construct such a special projection. In this chapter, we formalize this intuition and extend it from density matrices d to states $\rho = (\rho_n)_n$. This extension from individual density matrices to states

involves studying the limiting behavior of the von Neumann entropy of ρ_n as n goes to infinity.

Our results may be summarized by the following implications: For any computable ρ,

$$\exists c > 0 \; \exists^{\infty} n \; H(\rho_n) > n - c \Rightarrow \rho \text{ is q-MLR} \Rightarrow H(\rho) := \lim_n \frac{H(\rho_n)}{n} = 1.$$

Further, we also show that these implications do not reverse.

Chapter 2

Notions of quantum algorithmic randomness

2.1 Introduction

This section has two major themes. First, it continues the study of quantum Martin-Löf randomness initiated by Nies and Scholz [31]. Second, we define quantum Solovay and quantum Schnorr randomness and prove results concerning these notions. Along with Martin-Löf randomness, Solovay randomness and Schnorr randomness are important classical randomness notions. While Solovay randomness is equivalent to MLR, Schnorr randomness is strictly weaker. In Section 2.2 we define quantum Solovay and quantum Schnorr randomness, show that quantum Solovay randomness is equivalent to q-MLR, show the convexity of the randomness classes in the space of states (answering open questions [30, 31]), and obtain results regarding q-MLR states. The equivalence of quantum Solovay and quantum Martin-Löf randomness turns out to be a corollary of Theorem 2.9, a linear algebraic result of independent interest concerning the approximation of density matrices by subspaces. This result, to the best of our knowledge, is novel and may prove useful in areas where approximations to density matrices are used; for example, quantum information and error correction, quantum Kolmogorov complexity [8, 26]

and quantum statistical mechanics.

In Section 2.3, we study states which are coherent sequences of diagonal density matrices. These states can be thought of as probability measures on Cantor space. Nies and Stephan [32] defined Martin-Löf absolutely continuity and Solovay randomness for diagonal states. We show that these two notions are the restrictions of q-MLR and quantum Solovay randomness to the space of diagonal states. We prove a result (Lemma 3.3) about approximating a subspace of small rank by another one with a different orthonormal spanning set and of appropriately small rank. This result, novel as far as we know, may be applied to the important problem of approximating an entangled subspace (a subspace spanned by entangled pure states) by one spanned by product tensors [13, 19]. We discuss how quantum randomness notions restrict to classical states (i.e., to infinite bitstrings) and note that quantum Schnorr randomness is strictly weaker that q-MLR, as in the classical case.

Nies and Tomamichel [29] showed that q-MLR states satisfy quantum versions of the law of large numbers and the Shannon–McMillan–Breiman theorem for i.i.d. Bernoulli measures. In Sections 2.4 and 2.5 we strengthen their results by showing that in fact, all quantum Schnorr random states (a set strictly containing the q-MLR states) satisfy these properties.

Many results in this chapter have significantly different proofs, which may be found in [11].

2.2 Notions of quantum algorithmic randomness

2.2.1 Solovay and Schnorr randomness

An infinite bitstring X is said to *pass* the Martin-Löf test $(U_n)_n$ if $X \notin \bigcap_n U_n$ and is said to be *Martin-Löf random (MLR)* if it passes all Martin-Löf tests. A related randomness notion is Solovay randomness. A computable sequence of Σ^0_1 classes, $(S_n)_n$ is a *Solovay test* if $\sum_n \mu(S_n)$, the sum of the Lebesgue measures is finite. An infinite bitstring X *passes* $(S_n)_n$ if $X \in S_n$ for infinitely many n. It is a remarkable fact that X is MLR if and only if it passes all Solovay tests. Is this also true in the quantum realm? Nies and Scholz asked [30] if there is a notion of a quantum Solovay test and if so, is quantum Martin-Löf randomness equivalent to passing all quantum Solovay tests. We answer this question in the affirmative by defining a quantum Solovay test and quantum Solovay randomness as follows. Roughly speaking, we obtain a notion of a quantum Solovay test by replacing 'Σ^0_1 class' and 'Lebesgue measure' in the definition of classical Solovay tests with 'quantum-Σ^0_1 set' and τ (Definition 1.7) respectively. We show below that quantum Solovay Randomness is equivalent to q-MLR.

Definition 2.1. A uniformly computable sequence of quantum-Σ^0_1 sets, $(S^k)_{k\in\omega}$ is a *quantum-Solovay test* if $\sum_{k\in\omega} \tau(S^k) < \infty$.

Definition 2.2. For $0 < \delta < 1$, a state ρ *fails the Solovay test* $(S^k)_{k\in\omega}$ *at level* δ if there are infinitely many k such that $\rho(S^k) > \delta$.

Definition 2.3. A state ρ *passes the Solovay test* $(S^k)_{k\in\omega}$ if for all $\delta > 0$, ρ does not fail $(S^k)_{k\in\omega}$ at level δ. I.e, $\lim_k \rho(S^k) = 0$.

Definition 2.4. A state ρ is *quantum Solovay random* if it passes all quantum Solovay tests.

An *interval Solovay test* [21] is a Solovay test, $(S_n)_n$ such that each S_n is generated by a finite collection of strings. The following two definitions are due to Nies (personal communication). The first is a quantum analogue of an interval Solovay test.

Definition 2.5. A *strong Solovay test* is a computable sequence of special projections $(S^m)_m$ such that $\sum_m \tau(S^m) < \infty$. A state ρ fails $(S^m)_m$ at ϵ if for infinitely many m, $\rho(S^m) > \epsilon$.

Definition 2.6. A state ρ is *weak Solovay random* if it passes all strong quantum Solovay tests.

By 7.2.22 in the book by Downey and Hirschfeldt [21], a Schnorr test may be defined as:

Definition 2.7. A *Schnorr test* is an interval Solovay test, $(S^m)_m$ such that $\sum_m \mu(S^m)$ is a computable real number.

A bitstring passes a Schnorr test if it does not fail it (using the same notion of failing as in the Solovay test). We mimic this notion in the quantum setting.

Definition 2.8. A *quantum Schnorr test* is a strong Solovay test, $(S^m)_m$ such that $\sum_m \tau(S^m)$ is a computable real number. A state is quantum Schnorr random if it passes all Schnorr tests.

2.2.2 A general result about density matrices

We prove a purely linear algebraic theorem about approximating density matrices by subspaces and then use it to show the equivalence of quantum Solovay and quantum Martin-Löf randomness in the next subsection.

In words, the theorem says the following. Let $\mathcal{F}$ be a set of subspaces of 'small' (at most d) total dimension and let Q be the set of density matrices 'δ close' to at least m many subspaces from $\mathcal{F}$. Then, there is a subspace of small (at most $6d/\delta m$) dimension '$\delta^2/72$ close' to every density matrix in Q .

Theorem 2.9. Let $m, d, n \in \mathbb{N}$ and $\delta \in (0,1)$ be arbitrary. Let $\mathcal{F} = (T_k)_k$ be a set of subspaces of $\mathbb{C}^n$ with $\sum_k \dim(T_k) \leqslant d$, and let M_k be the orthonormal projection onto T_k. Let

$$Q = \{\rho : \rho \text{ is a density matrix on } \mathbb{C}^n \text{with } \mathrm{Tr}(\rho M_k) > \delta \text{ for at least } m \text{ many } k\},$$

be non-empty. Then, there is a orthonormal projection matrix M such that

$$\mathrm{Tr}(M) \leqslant \frac{6d}{\delta m} \text{ and } \mathrm{Tr}(M\rho) \geqslant \frac{\delta^2}{36} \text{ for every } \rho \in Q.$$

Proof. Let

$$L = \left\{ \psi \in \mathbb{C}^n : ||\psi|| = 1, \sum_k \mathrm{Tr}(|\psi\rangle\langle\psi| M_k) > \frac{m\delta}{6} \right\},$$

and let D be a maximal orthonormal subset of L and let M be the orthonormal projection matrix onto the span of D.

Lemma 2.10. $\mathrm{Tr}(M) \leqslant \dfrac{6d}{\delta m}$.

Proof. We prove this using that D is a orthonormal subset of L, that $\mathrm{Tr}(M) = |D|$ and

that d bounds the sum of the dimensions.

$$d \geqslant \sum_k \mathrm{Tr}(M_k) \geqslant \sum_k \sum_{\psi \in D} \mathrm{Tr}(|\psi\rangle\langle\psi| M_k) = \sum_{\psi \in D} \sum_k \mathrm{Tr}(|\psi\rangle\langle\psi| M_k)$$
$$> |D| \frac{m\delta}{6} = \mathrm{Tr}(M) \frac{m\delta}{6}. \square$$

Take any $\rho \in Q$. We can write it as

$$\rho = \sum_{i \leqslant n} \alpha_i |\psi^i\rangle\langle\psi^i|$$

for α_i non-negative real numbers with $\sum_{i \leqslant n} \alpha_i = 1$ and for each i, $|\psi^i\rangle \in \mathbb{C}^n$ and $||\psi^i|| = 1$. For any $i \leqslant n$ we can decompose $\psi = \psi^i$ as

$$\psi = c_o \psi_o + c_p \psi_p \tag{2.1}$$

where $\psi_o \in \mathrm{range}(M)$ and $\psi_p \in \mathrm{range}(M)^\perp$ are unit vectors and $c_o, c_p \in \mathbb{C}$ satisfy $|c_0|^2 + |c_p|^2 = 1$. We now show that $\dfrac{\delta^2}{36} \leqslant \mathrm{Tr}(\rho M) = \sum_{i \leqslant n} \alpha_i |c_o^i|^2$. Let k be arbitrary and let $M_k = S$. A routine computation gives,

$$\mathrm{Tr}(S|\psi\rangle\langle\psi|) \tag{2.2}$$
$$\leqslant |c_o|^2 \langle S\psi_o | S\psi_o\rangle + |c_p|^2 \langle S\psi_p | S\psi_p\rangle + 2|c_o||c_p| |\langle S\psi_p | S\psi_o\rangle|. \tag{2.3}$$

By the Cauchy-Schwarz inequality:

$$|\langle S\psi_p | S\psi_o\rangle| \leqslant ||S\psi_o|| ||S\psi_p||$$
$$\leqslant (\max\{||S\psi_o||, ||S\psi_p||\})^2$$
$$\leqslant ||S\psi_o||^2 + ||S\psi_p||^2.$$

Putting this in 2.2, we have:

$$\mathrm{Tr}(S|\psi\rangle\langle\psi|) \tag{2.4}$$

$$\leqslant |c_o|^2\langle S\psi_o|S\psi_o\rangle + |c_p|^2\langle S\psi_p|S\psi_p\rangle + 2|c_o||c_p|(||S\psi_o||^2 + ||S\psi_p||^2) \tag{2.5}$$

$$\leqslant |c_o|\langle S\psi_o|S\psi_o\rangle + |c_p|\langle S\psi_p|S\psi_p\rangle + 2|c_o|||S\psi_o||^2 + 2|c_p|||S\psi_p||^2 \tag{2.6}$$

$$= 3(|c_o|\langle S\psi_o|S\psi_o\rangle + |c_p|\langle S\psi_p|S\psi_p\rangle). \tag{2.7}$$

As $\rho \in Q$, pick H such that $|H| = m$ and $\mathrm{Tr}(\rho M_k) > \delta$ for each k in H. Using the above,

$$\begin{aligned} m\delta &< \sum_{k\in H} \mathrm{Tr}(\rho M_k) \\ &= \sum_{i\leqslant n} \alpha_i \sum_{k\in H} \mathrm{Tr}(|\psi^i\rangle\langle\psi^i|M_k) \\ &\leqslant \sum_{i\leqslant n} \alpha_i \sum_{k\in H} 3(|c_o^i|\langle M_k\psi_o^i|M_k\psi_o^i\rangle + |c_p^i|\langle M_k\psi_p^i|M_k\psi_p^i\rangle). \end{aligned}$$

So,

$$\frac{m\delta}{3} \leqslant \sum_{i\leqslant n} \alpha_i \sum_{k\in H} (|c_o^i|\langle M_k\psi_o^i|M_k\psi_o^i\rangle + |c_p^i|\langle M_k\psi_p^i|M_k\psi_p^i\rangle) \tag{2.8}$$

$$= \sum_{i\leqslant n} \alpha_i|c_o^i| \sum_{k\in H} \langle M_k\psi_o^i|M_k\psi_o^i\rangle + \sum_{i\leqslant n} \alpha_i|c_p^i| \sum_{k\in H} \langle M_k\psi_p^i|M_k\psi_p^i\rangle. \tag{2.9}$$

Recall that our goal was to bound $\sum_{i\leqslant n} \alpha_i|c_o^i|^2$ from below by $\delta^2/36$. In what follows, we achieve this by observing that the maximality of D implies that $\psi_p^i \notin L$.

Fix an arbitrary i and recall that $\psi_p^i \in \mathrm{range}(M)^\perp$. Hence, ψ_p^i is perpendicular to each element of D. If, $\psi_p^i \in L$, then $\{\psi_p^i\} \cup D$ is a orthonormal subset of L strictly containing D, contradicting the maximality of D. So, for each i it must be that $\psi_p^i \notin L$.

But $||\psi_p^i|| = 1$. This implies that for each i,

$$\sum_k \mathrm{Tr}(|\psi_p^i\rangle\langle\psi_p^i|M_k) \leqslant \frac{m\delta}{6}. \tag{2.10}$$

As $\sum_{i\leqslant n} \alpha_i = 1$ and $|c_p^i| \leqslant 1$, the second term in 2.9 can be bounded from above:

$$\sum_{i\leqslant n} \alpha_i |c_p^i| \sum_{k\in H} \langle M_k\psi_p^i|M_k\psi_p^i\rangle \leqslant \frac{m\delta}{6}. \tag{2.11}$$

Also note that

$$\sum_{k\in H} \langle M_k\psi_o^i|M_k\psi_o^i\rangle \leqslant m. \tag{2.12}$$

2.9, 2.11 and 2.12 imply that

$$\frac{\delta}{6} \leqslant \sum_{i\leqslant n} \alpha_i |c_o^i|.$$

By Jensen's inequality,

$$\frac{\delta^2}{36} \leqslant \big(\sum_{i\leqslant n} \alpha_i |c_o^i|\big)^2 \leqslant \sum_{i\leqslant n} \alpha_i |c_o^i|^2. \tag{2.13}$$

Finally,

$$\begin{aligned}
\mathrm{Tr}(\rho_n M) &= \sum_{i\leqslant n} \alpha_i \mathrm{Tr}(|\psi^i\rangle\langle\psi^i|M) \\
&= \sum_{i\leqslant n} \alpha_i \mathrm{Tr}(|M\psi^i\rangle\langle M\psi^i|) \\
&= \sum_{i\leqslant n} \alpha_i \mathrm{Tr}(|c_o^i\psi_o^i\rangle\langle c_o^i\psi_o^i|) \\
&= \sum_{i\leqslant n} \alpha_i |c_o^i|^2 \geqslant \frac{\delta^2}{36}.\square
\end{aligned}$$

2.2.3 Quantum Solovay randomness is equivalent to quantum Martin-Löf randomness

Theorem 2.11. A state is quantum Solovay random if and only if it is quantum Martin-Löf random.

Proof. It suffices to show that if a state ρ is not quantum Solovay random then it is not quantum Martin-Löf random. To this end, let $\rho = (\rho_n)_{n\in\omega}$ be a state which fails a quantum Solovay test, $(S^k)_{k\in\omega}$ at level δ. We show that ρ is not quantum Martin-Löf random by building a quantum Martin-Löf test, $(G^m)_{m\in\omega}$, with $G^m = (G^m_n)_{n\in\omega}$, which ρ fails at level $\delta^2/72$. We will use an effective version of Theorem 2.9 . Without loss of generality, assume that $S^k_n = \varnothing$ for $k > n$ and let $\sum_k \tau(S^k) < 1$. We use the notation:

$$A^m_t = \left\{ \psi \in \mathbb{C}^{2^t}_{alg} : ||\psi|| = 1, \sum_{k\leqslant t} \mathrm{Tr}(|\psi\rangle\langle\psi| S^k_t) > \frac{2^m\delta}{6} \right\},$$

for $t, m \in \omega$. This is analogous to L in 2.9 with the replacements, $m \mapsto 2^m, n \mapsto 2^t$ and $d \mapsto 2^n$ and where we restrict attention to algebraic vectors. We use A instead of L to emphasize that we only consider complex algebraic objects in A, a 'computable' version of L

Construction of G^m: We build G^m inductively as follows. Given $C^m_{n-1} \subseteq \mathbb{C}^{2^{n-1}}_{alg}$, a maximal (under set inclusion) orthonormal subset of A^m_{n-1}, let

$$D^m_n = \left\{ |\psi\rangle \otimes |i\rangle \in \mathbb{C}^{2^n}_{alg} : i \in \{1, 0\}, \psi \in C^m_{n-1} \right\}.$$

Note that $D^m_n \subseteq A^m_n$ since $C^m_{n-1} \subseteq A^m_{n-1}$. Define C^m_n to be S where S is a maximal orthonormal set such that $S \subseteq A^m_n$ and $D^m_n \subseteq S$. Let G^m_n be the projection:

$$G^m_n = \sum_{\psi\in C^m_n} |\psi\rangle\langle\psi|.$$

End of construction.

Lemma 2.12. $(G^m)_{m\in\omega}$ is a quantum Martin-Löf test.

Proof. Fix m. Clearly, $(C^m_n)_{n\in\omega}$ is a uniformly computable sequence. By construction, $\text{range}(G^m_{n-1}\otimes I_2) \subseteq \text{range}(G^m_n)$. So, $G^m = (G^m_n)_{n\in\omega}$ is a quantum-Σ^0_1 set for each m. The sequence $(G^m)_{m\in\omega}$ is uniformly computable in m by construction. Since, $1 \geqslant \sum_k \tau(S^k)$, we have that $2^n \geqslant \sum_k \text{Tr}(S^k_n)$ for all n. Now make the replacements $m \mapsto 2^m, n \mapsto 2^n$ and $d \mapsto 2^n$ in the proof of 2.10 to see that $\text{Tr}(G^m_n) \leqslant (6/\delta)2^{n-m}$ for all m, n. So $\tau(G^m) \leqslant (6/\delta)2^{-m}$ for all m. □

Lemma 2.13. ρ fails $(G^m)_m$ at level $\dfrac{\delta^2}{72}$.

Proof. We must show that $\inf_{m\in\omega}\rho(G^m) > \dfrac{\delta^2}{72}$. It suffices to show that for all $m \in \omega$, there is an n such that $\text{Tr}(\rho_n G^m_n) > \dfrac{\delta^2}{72}$. To this end, let m be arbitrary and fix a n big enough so that there exist 2^m many ks such that $\text{Tr}(\rho_n S^k_n) > \delta$. So, let $|H| = 2^m$ and $\text{Tr}(\rho_n S^k_n) > \delta$ for each k in H. The projection G^m_n will play the role of M in the proof of Theorem 2.9. Write ρ_n as

$$\rho_n = \sum_{i\leqslant 2^n} \alpha_i |\psi^i\rangle\langle\psi^i|$$

for α_i non-negative real numbers with $\sum_{i\leqslant 2^n} \alpha_i = 1$ and for each i, $|\psi^i\rangle \in \mathbb{C}^{2^n}$ and $||\psi^i|| = 1$. First, consider the case where $|\psi^i\rangle \in \mathbb{C}^{2^n}_{alg}$ for all i. For any $i \leqslant 2^n$ we can decompose $\psi = \psi^i$ as,

$$\psi = c_o\psi_o + c_p\psi_p$$

as in the proof of Theorem 2.9, which we mimic now. By equation 2.9,

$$\frac{2^m\delta}{3} \leqslant \sum_{i\leqslant 2^n} \alpha_i|c^i_o| \sum_{k\in H} \langle S^k_n\psi^i_o|S^k_n\psi^i_o\rangle + \sum_{i\leqslant 2^n} \alpha_i|c^i_p| \sum_{k\in H} \langle S^k_n\psi^i_p|S^k_n\psi^i_p\rangle \tag{2.14}$$

Fix an arbitrary i and recall that $\psi_p^i \in \text{range}(G_n^m)^\perp \cap \mathbb{C}_{alg}^{2^n}$. Hence, ψ_p^i is perpendicular to each element of C_n^m. If $\psi_p^i \in A_n^m$, then $\{\psi_p^i\} \cup C_n^m$ is a orthonormal subset of A_n^m strictly containing C_n^m, contradicting the maximality of C_n^m. So, for each i it must be that $\psi_p^i \notin A_n^m$. But, $\psi_p^i \in \mathbb{C}_{alg}^{2^n}$ and $||\psi_p^i|| = 1$. This implies that for each i,

$$\sum_{k \leqslant n} \text{Tr}(|\psi_p^i\rangle\langle\psi_p^i|S_n^k) \leqslant \frac{2^m\delta}{6}.$$

We are now in the situation of equation 2.10. As the argument following it does not need complex algebraic vectors and by recalling that M is replaced by G_n^m, we see that $\text{Tr}(\rho_n G_n^m) \geqslant \delta^2/36 > \delta^2/72$. Now, suppose that not all $|\psi^i\rangle$ are algebraic. By the density of $\mathbb{C}_{alg}^{2^n}$ in $\mathbb{C}^{2^n}$ we can approximate ρ_n by a sequence $(\pi_k)_{k\in\mathbb{N}}$ of density matrices each satisfying the conditions of the previous case. So, $\text{Tr}(\pi_k G_n^m) \geqslant \delta^2/36$. By continuity, $\text{Tr}(\rho_n G_n^m) \geqslant \delta^2/36 > \delta^2/72$. □ □

The theorem is proved. □ □

2.2.4 Convexity

We show that all classes of random states are convex. The first result in this section is a corollary of the main theorem from the previous section.

Corollary 2.14. A convex combination of q-Martin-Löf random states is q-Martin-Löf random. Formally, if $(\rho^i)_{i<k<\omega}$ are q-ML random states and $\sum_{i<k<\omega} \alpha_i = 1$, then $\rho = \sum_{i<k} \alpha_i \rho^i$ is q-ML random.

Proof. Suppose for a contradiction that there is a q-Martin-Löf test $(G^m)_{m\in\omega}$ and a $\delta > 0$ such that $\forall m \in \omega$, $\rho(G^m) > \delta$. So, $\forall m \in \omega$, $\exists n$ such that $\text{Tr}(\rho_n G_n^m) > \delta$ where

$\rho_n = \sum_{i<k} \alpha_i \rho_n^i$. So, $\forall m \in \omega$, $\exists n$ such that

$$\delta < \mathrm{Tr}\left(\sum_{i<k} \alpha_i \rho_n^i G_n^m \right) = \sum_{i<k} \alpha_i \mathrm{Tr}(\rho_n^i G_n^m).$$

By convexity of the sum, there is an i such that $\mathrm{Tr}(G_n^m \rho_n^i) > \delta$. In summary,

$$\forall m, \text{ there is an } i \text{ and an } n \text{ such that } \mathrm{Tr}(\rho_n^i G_n^m) > \delta.$$

Since there are only finitely many is, by the pigeonhole principle, there is an i such that $\exists^\infty m$ with Tr $(\rho_n^i G_n^m) > \delta$, for some n. So, $\exists^\infty m$ with $\rho^i(G^m) > \delta$. So, ρ^i fails the q-Solovay test $(G^m)_{m\in\omega}$ and hence is not q-Martin-Löf random by our previous result. This is a contradiction. □

Theorem 2.15. A convex combination of quantum Schnorr random states is quantum Schnorr random. Formally, if $(\rho^i)_{i<k<\omega}$ are quantum Schnorr random states and $\sum_{i<k<\omega} \alpha_i = 1$, then $\rho = \sum_{i<k} \alpha_i \rho^i$ is quantum Schnorr random.

Proof. Suppose for a contradiction that there is a quantum Schnorr test $(G^m)_{m\in\omega}$ and a $\delta > 0$ such that $\exists^\infty m \in \omega$, $\rho(G^m) > \delta$. Letting G^m be n_m by n_m, $\exists^\infty m$, such that

$$\delta < \mathrm{Tr}(\rho_{n_m} G_{n_m}^m) = \mathrm{Tr}(\sum_{i<k} \alpha_i \rho_{n_m}^i G_{n_m}^m) = \sum_{i<k} \alpha_i \mathrm{Tr}(\rho_{n_m}^i G_{n_m}^m).$$

By convexity of the sum, there is an i such that $\mathrm{Tr}(G_{n_m}^m \rho_{n_m}^i) > \delta$. In summary,

$$\exists^\infty m, \text{ there is an } i \text{ such that } \mathrm{Tr}(\rho_{n_m}^i G_{n_m}^m) > \delta.$$

Since there are only finitely many i s, by the pigeonhole principle, there is an i such that $\exists^\infty m$ with Tr $(\rho_{n_m}^i G_{n_m}^m) > \delta$. So, $\exists^\infty m$ with $\rho^i(G^m) > \delta$. So, ρ^i fails the q-Schnorr test $(G^m)_{m\in\omega}$ and hence is not q-Schnorr. This is a contradiction. □

Noting that the above proof needed only the Solovay type of failing criterion, we get:

Theorem 2.16. A convex combination of weak Solovay random states is q-weak Solovay random. Formally, if $(\rho^i)_{i<k<\omega}$ are weak Solovay random states and $\sum_{i<k<\omega} \alpha_i = 1$, then $\rho = \sum_{i<k} \alpha_i \rho^i$ is weak Solovay random.

The proof is almost identical to the previous one.

2.2.5 Nesting property of quantum Martin-Löf tests

It is interesting to see which classical results carry over to the quantum realm. For example, the existence of a universal MLT, $(U_n)_n$ such that a bitstring is MLR if and only if it passes this $(U_n)_n$ does carry over [31]. The 'nesting property' of the classical Martin-Löf test says that we can, without loss of generality assume the universal test $(U_n)_n$ to be nested; i.e., to satisfy $U_{n+1} \supseteq U_n$ for all n. We extend this property to the quantum setting:

Theorem 2.17. There is a q-MLT, $(Q^m)_{m\in\mathbb{N}}$ with the properties (1) If a state ρ fails the universal q-Martin-Löf test $(G^m)_{m\in\mathbb{N}}$ at $\delta > 0$, then, it also fails $(Q^m)_{m\in\mathbb{N}}$ at $\delta > 0$ (2) If $Q^m = (Q^m_n)_{n\in\mathbb{N}}$ for all m, then for all m and n, range$(Q^{m+1}_n) \subseteq$ range (Q^m_n). In particular, $Q^{m+1} \leqslant Q^m$ for all m.

Proof. Informally speaking, we want to let Q^m be $\sum_{i>m} G^i$. Precisely, we build Q^m level by level. For any natural numbers $i \leqslant n$, let

$$G^i_n = \sum_{j=1}^{2^{n-i}} |v^{i,n}_j\rangle\langle v^{i,n}_j|.$$

Let

$$S^m_n := \text{span} \bigcup_{i=m}^{n} \{v^{i,n}_j : 1 \leqslant j \leqslant 2^{n-i}\},$$

and let Q^m_n be the special projection onto S^m_n. Let $Q^m = (Q^m_n)_n$. Fix an m. We see that $Q^m_n \leqslant Q^m_{n+1}$, since $G^i_n \leqslant G^i_{n+1}$ holds for all i, n. So, Q^m is a q-Σ^0_1 class. The dimension of S^m_n is at most $\sum_{i=m}^n \mathrm{Trace}(G^i_n) \leqslant \sum_{i=m}^n 2^{n-i} < 2^{n-m+1}$. So, $(Q^m)^\infty_{m=2}$ is a q-MLT. Let m and n be arbitrary and $n \geqslant m+1$. Then, clearly, by definition of S^m_n, we see that range$(Q^{m+1}_n) \subseteq$ range (Q^m_n). So, the nesting property holds. Let $\rho = (\rho_n)_n$ be a state. By the nesting, and by properties of projection operators, we have that for a fixed m and all n,

$$\mathrm{Tr}(\rho_n Q^{m+1}_n) \leqslant \mathrm{Tr}(\rho_n Q^m_n) \leqslant \rho(Q^m).$$

So, $\rho(Q^{m+1}) = \sup_n \mathrm{Tr}(\rho_n Q^{m+1}_n) \leqslant \rho(Q^m)$ for all m. (1) clearly holds. □

2.3 Randomness for diagonal states

A state $\rho = (\rho_n)_n$ is defined to be *diagonal* if ρ_n is diagonal for all n. So, each ρ_n in a diagonal state represents a mixture of separable states. A diagonal $\rho = (\rho_n)_n$ can be thought of as a measure on Cantor space, denoted by μ_ρ: if $\sigma \in 2^n$, we define $\mu_\rho([\![\sigma]\!]) := \langle \sigma|\rho_n|\sigma\rangle$. We will write $\mu_\rho(\sigma)$ instead of $\mu_\rho([\![\sigma]\!])$. μ_ρ is easily seen to be a measure by noting that the partial trace over the last qubit of ρ_{n+1} equals ρ_n for all n. Recalling the notation in Remark 1.12 and as S is prefix free, we have,

$$\mu_\rho([\![S]\!]) = \sum_{\sigma \in S} \mu_\rho(\sigma) = \sum_{\sigma \in S} \langle \sigma|\rho_n|\sigma\rangle = \mathrm{Tr}(\rho_n P_S).$$

This will be used frequently. Nies and Stephan have recently defined a notion of randomness for measures on Cantor space called Martin-Löf absolute continuity [32].

Definition 2.18. A measure π on Cantor space is called *Martin-Löf absolutely continuous* if $\inf_m \pi(G_m) = 0$ for each classical MLT $(G_m)_{m \in \mathbb{N}}$.

This notion turns out to be equivalent to quantum Martin-Löf randomness in the sense that for a diagonal ρ, ρ is q-MLR if and only if μ_ρ is Martin-Löf absolutely continuous. It is easy to see that if a diagonal ρ is q-MLR, then μ_ρ is Martin-Löf absolutely continuous. We now show the other direction.

Theorem 2.19. Let ρ be diagonal. If it fails a q-MLT $(G^m)_{m\in\mathbb{N}}$ at order δ, then there is a classical MLT, $(C^m)_{m\in\mathbb{N}}$ such that $\inf_m \mu_\rho(C^m) > \delta/2$.

Proof. We isolate here a simple but useful property.

Lemma 2.20. Let n be a natural number, $E = (e_i)_{i=1}^{2^n}$ be any orthonormal basis for $\mathbb{C}^{2^n}$ and F be any hermitian, orthonormal projection matrix acting on $\mathbb{C}^{2^n}$. For any $\delta > 0$, let

$$S^\delta_{E,F} := \left\{ e_i \in E : \left\langle e_i|F|e_i \right\rangle > \delta \right\}.$$

Then, $|S^\delta_{E,F}| < \delta^{-1}\mathrm{Tr}(F)$.

Proof. Note that since F is a hermitian orthonormal projection, $\left\langle e_i|F|e_i \right\rangle = \left\langle Fe_i|Fe_i \right\rangle = |Fe_i|^2 \geqslant 0$. So,

$$\delta|S^\delta_{E,F}| < \sum_{e_i\in S^\delta_{E,F}} \left\langle e_i|F|e_i \right\rangle \leqslant \sum_{i\leqslant 2^n} \left\langle e_i|F|e_i \right\rangle = \mathrm{Tr}(F).$$

□

We now prove Theorem 2.19. The intuition is as follows: given a special projection, we take the set of bitstrings (thought of as qubitstrings) 'close' to it. If the special projection 'captures' δ much mass of ρ, then the projection onto the span of these qubitstrings must capture atleast $\delta/2$ much mass of ρ. σ will always denote a finite length classical bit string and $|\sigma\rangle$, the corresponding element of the standard computational

basis. We may assume that δ is rational. Fix m. We describe the construction of $C^m = (C^m_n)_{n\in\mathbb{N}}$ (See 1.6). Let

$$T^m_n := \left\{\sigma \in 2^n : \langle \sigma | G^m_n | \sigma \rangle > \frac{\delta}{4}\right\}.$$

These are those standard basis vectors 'close' to G^m_n. Let

$$C^m_n = \bigcup_{\sigma\in T^m_n} [\![\sigma]\!].$$

Lemma 2.21. C^m is a Σ^0_1 class for any m.

Proof. It is easy to see that for all $\sigma \in T^m_n$ and $i \in \{0,1\}$,

$$\langle \sigma i | G^m_{n+1} | \sigma i \rangle \geqslant \langle \sigma | G^m_n | \sigma \rangle > \frac{\delta}{4}.$$

So, $\{\sigma i : \sigma \in T^m_n, i \in \{0,1\}\} \subseteq T^m_{n+1}$. Also note that T^m_n is uniformly computable in n since G^m_n is. □

Lemma 2.22. $(C^m)_{m\in\mathbb{N}}$ is a MLT.

Proof. Fix m. Letting $E = B^n$ and $F = G^m_n$ in Lemma 3.3 and by definition of q-MLT,

$$|T^m_n| < \frac{4}{\delta} 2^n \tau(G^m) \leqslant \frac{4}{\delta} 2^{n-m}.$$

So, $\mu(C^m) < 2^{-m}\frac{4}{\delta}$. C^m is computable in m since G^m is. □

Now we show that $\inf_m \mu_\rho(C^m) > \delta/2$. Fix a m and a n (depending on m) such that $\mathrm{Tr}(\rho_n G^m_n) > \delta$. Let $\rho_n = \sum_{\sigma\in 2^n} \alpha_\sigma |\sigma\rangle\langle\sigma|$. Then,

$$\delta < \mathrm{Tr}(\rho_n G^m_n) = \sum_{\sigma\in 2^n} \alpha_\sigma \langle \sigma | G^m_n | \sigma \rangle = \sum_{\sigma\in T^m_n} \alpha_\sigma \langle \sigma | G^m_n | \sigma \rangle + \sum_{\sigma\in 2^n\setminus T^m_n} \alpha_\sigma \langle \sigma | G^m_n | \sigma \rangle$$

$$\leqslant \sum_{\sigma\in T^m_n} \alpha_\sigma + \sum_{\sigma\in 2^n\setminus T^m_n} \alpha_\sigma \frac{\delta}{4} \leqslant \sum_{\sigma\in T^m_n} \alpha_\sigma + \frac{\delta}{4} = \mathrm{Tr}(\rho_n P_{C^m_n}) + \frac{\delta}{4} = \mu_\rho(C^m_n) + \frac{\delta}{4}.$$

The last equality follows as T^m_n is prefix free. So, $\mu_\rho(C^m) \geqslant \mu_\rho(C^m_n) \geqslant 3\delta/4$. □

Nies and Scholz showed that a measure, μ is Martin-Löf absolutely continuous if and only if for any Solovay test $(S_k)_k$, $\lim_k \mu(S_k) = 0$ [32]. Adapting the proof of Theorem 2.11 yields another proof of this.

Theorem 2.23. Let ρ be diagonal. If for some Solovay test $(S_k)_k$ and $\delta > 0$ we have $\exists^\infty k, \mu_\rho(S_k) > \delta$, then there is a Martin-Löf test $(J_m)_m$ such that $\inf_m \mu_\rho(J^m) > \delta/2$.

The theorem will follow from the two lemmas below. Write $S^k = (S^k_n)_n$ as in Definition 1.6. Without loss of generality, let $S^k_n = \varnothing$ for $k > n$. Let

$$C^m_t = \left\{ \sigma \in 2^t : \sum_{k \leqslant t} |\langle \sigma | S^k_t | \sigma \rangle| > 2^{m-1}\delta \right\},$$

and let $G^m_t := P_{C^m_t}$ (See Remark 1.12). Let $G^m = (G^m_n)_n$. It is easy to see that G^m is a q-Σ^0_1 set for each m. Let $J^m_n := [\![C^m_n]\!]$ and $J^m = (J^m_n)_n$. One can check that that $(J^m)_m$ is a MLT if and only if $(G^m)_m$ is quantum Martin-Löf test. So, $(J^m)_m$ is a MLT since:

Lemma 2.24. $(G^m)_m$ is quantum Martin-Löf test.

Proof. Identical to the proof of 2.10. □

Lemma 2.25. We have that $\inf_m \mu_\rho(J^m) > \delta/2$.

Proof. Let m be arbitrary. By assumption, there are infinitely many ks such that $\mu_\rho(S^k) > \delta$. For each of these, there is an n such that $\mu_\rho(S^k_n) > \delta$. So, fix a n so that there are 2^m many ks such that $\mu_\rho(S^k_n) > \delta$. Since ρ_n is diagonal, let

$$\rho_n = \sum_{\sigma \in 2^n} \alpha_\sigma |\sigma\rangle\langle\sigma|.$$

By the choice of n, pick $M \subseteq \{1, 2 \cdots, n\}$ such that $|M| = 2^m$ and $\mu_\rho(S^k_n) > \delta$ for each k in M. Note that $\mu_\rho(S^k_n) = \mathrm{Tr}(\rho_n P_{S^k_n})$, since S^k_n is prefix free. We write $\mathrm{Tr}(\rho_n P_{S^k_n}) = \mathrm{Tr}(\rho_n S^k_n)$ to avoid clutter. So,

$$
\begin{aligned}
2^m\delta &< \sum_{k\in M} \mu_\rho(S^k_n) = \sum_{k\in M} \mathrm{Tr}(\rho_n S^k_n) = \sum_{\sigma\in 2^n} \alpha_\sigma \sum_{k\in M} \mathrm{Tr}(|\sigma\rangle\langle\sigma|S^k_n) \\
&= \sum_{\sigma\in C^m_n} \alpha_\sigma \sum_{k\in M} \langle\sigma|S^k_n\sigma\rangle + \sum_{\sigma\notin C^m_n} \alpha_\sigma \sum_{k\in M} \langle\sigma|S^k_n\sigma\rangle \\
&\leqslant \sum_{\sigma\in C^m_n} \alpha_\sigma \sum_{k\in M} \langle\sigma|S^k_n\sigma\rangle + 2^{m-1}\delta \\
&\leqslant 2^m \sum_{\sigma\in C^m_n} \alpha_\sigma + 2^{m-1}\delta.
\end{aligned}
$$

The second last inequality follows from the definition of G^m_n and convexity; the last from the choice of M. Finally, we get that,

$$
\delta/2 < \sum_{\sigma\in C^m_n} \alpha_\sigma = \mu_\rho([\![C^m_n]\!]) \leqslant \mu_\rho(J^m).
$$

□

Next, we discuss a subset of the diagonal states; the Dirac delta measures on Cantor space.

2.3.1 Quantum randomness on Cantor Space

A classical bitstring can be thought of as a diagonal state: If X is a real in Cantor space, the state $\rho_X = (\rho_n)_n$ given by $\rho_n = |X \upharpoonright n\rangle\langle X \upharpoonright n|$ is the quantum analog of X. Do the quantum randomness notions agree with classical notions when restricted to Cantor space? By Theorem 2.19, we see that ρ_X is q-MLR if and only if X is MLR. Further, ρ_X is q-MLR if and only if ρ_X is weak Solovay random. Also, X is MLR if and only if it passes all interval Solovay tests (the classical analog of strong Solovay tests). So, we see that q-MLR and weak Solovay randomness agree with the classical versions on Cantor space. What about quantum Schnorr randomness?

Lemma 2.26. ρ_X is quantum Schnorr random if and only if X is Schnorr random.

Proof. Let $(Q^r)_r$ be a quantum Schnorr test which ρ_X fails at some rational δ. Let Q^r be n_r by n_r. Using notation of Lemma 3.3, let $T^r := S^{\delta}_{E,Q^r}$ where E is the set of length n_r standard basis vectors. We think of T^r as a set of classical bitstrings. By Lemma 3.3, $\tau(T^r) \leqslant \delta^{-1}\tau(Q^r)$. So, $\sum_r 2^{-n_r}|T^r| = \sum_r \tau(T^r) \leqslant \delta^{-1}\sum_r \tau(Q^r)$ is computable because $\sum_r \tau(Q^r)$ is. So, $(T^r)_r$ is a finite total Solovay test. Let m be one of the infinitely many r such that $\delta <\mathrm{Tr}(\rho_X(Q^r))$. Then, by definition, $X \upharpoonright n_r$ is in T^r. So, X fails $(T_r)_r$ and hence is not Schnorr random (by 7.2.21 and 7.2.22 in the book by Downey and Hirschfeldt [21]). The other direction is trivial. □

2.3.2 Relating the randomness notions

We have seen that

$$\text{Solovay R} = \text{q-MLR} \subseteq \text{weak Solovay R} \subset \text{quantum Schnorr R}.$$

The equality follows by Theorem 2.11. The second inclusion is strict as there is a bitstring which is Schnorr random but which fails some interval Solovay test [21] and since by Theorem 2.26, this bitstring must be quantum Schnorr random. It is open whether the first inclusion is strict.

2.4 A law of large numbers for quantum Schnorr randoms

The law of large numbers (LLN), specialized to Cantor space says that the limiting proportion of ones is equal to 0.5 for almost every bitstring. Random bitstrings satisfy

the LLN. In fact, satisfying the LLN is the weakest form of randomness [21]. This is quite intuitive; one would not call a bitstring 'random' if it has more ones than zeroes in the limit. Analogously, we expect even our weakest notion of quantum randomness (quantum Schnorr randomness) to satisfy a quantum analogue of the LLN. This suggests that the quantum randomness notions are 'natural' and mirror the classical situation. In this section, σ will always denote a classical bitstring thought of as a qubit string.

Definition 2.27. [29] *ρ satisfies the LLN* if $\lim_n n^{-1}\sum_{i<n}\mathrm{Tr}(\rho_n P_i^n) = 0.5$, where for all $i \geqslant 0, n > 0$,

$$P_i^n := \sum_{\sigma:|\sigma|=n,\sigma(i)=1} |\sigma\rangle\langle\sigma|.$$

The intuition is that P_i^n is the projection observable which measures whether a given density matrix on n qubits 'has a one in the i^{th} spot'. $\mathrm{Tr}(\rho_n P_i^n)$ is the probability that ρ_n 'has a one in the i^{th} spot'. If the average over i of these probabilities tends to 0.5 as n goes to infinity, then the state satisfies the LLN.

Theorem 2.28. Quantum Schnorr random states satisfy the LLN.

Proof. We prove it by contradiction. Suppose ρ is quantum Schnorr random but does not satisfy the LLN. So, there is a δ such that either $\exists^\infty n$, with $n^{-1}\sum_{i<n}\mathrm{Tr}(\rho_n P_i^n) > \delta + 0.5$ or $\exists^\infty n$, with $n^{-1}\sum_{i<n}\mathrm{Tr}(\rho_n P_i^n) < -\delta + 0.5$. Suppose first that the former holds. A rough outline of this proof is as follows. For each n we take S_n to be the subspace spanned by the classical strings with the fraction of 1s more than $0.5 + \delta/2$. $(S_n)_n$ is easily seen to be a quantum Schnorr test and it only remains to show that ρ fails it. This is not obvious as ρ is not necessarily classical, while $(S_n)_n$ is composed of classical vectors. To show this, we consider one of the infinitely many ns such that $n^{-1}\sum_{i<n}\mathrm{Tr}(\rho_n P_i^n) > \delta + 0.5$. For such an n, we break up $n^{-1}\sum_{i<n}\mathrm{Tr}(\rho_n P_i^n)$ into two parts: the first corresponding to

the projection of ρ_n onto $S_n^{\perp}$ and the other corresponding to the projection onto S_n (see for example in equation 2.29). The definition of S_n enables us to upper bound the first part (see 2.30). The second part is forced to be big since $n^{-1}\sum_{i<n}\mathrm{Tr}(\rho_n P_i^n) > \delta + 0.5$. So, ρ fails $(S_n)_n$. The details are: Define for all n,

$$C_n = \left\{\sigma : |\sigma| = n, n^{-1}\sum_{i<n} |\langle\sigma|P_i^n|\sigma\rangle| > \delta/2 + 0.5\right\}.$$

In other words,

$$C_n = \left\{\sigma : |\sigma| = n, n^{-1}|\{i < n : \sigma(i) = 1| > \delta/2 + 0.5\right\}.$$

Let S_n be the special projection,

$$S_n := \sum_{\sigma\in C_n} |\sigma\rangle\langle\sigma|.$$

$(S_n)_n$ is a computable sequence since we may let δ be rational. By the Chernoff bound, $\tau(S_n) = 2^{-n}|C_n| \leqslant 2\exp(-0.5n\delta^2)$ for all n. So, $\sum_n \tau(S_n)$ is computable showing that $(S_n)_n$ is a quantum Schnorr test.

For all n, let

$$\rho_n = \sum_{k<2^n} \alpha_k |\psi_n^k\rangle\langle\psi_n^k|$$

for α_k non-negative real numbers with $\sum_{k<2^n}\alpha_k = 1$ and for each k, $|\psi_n^k\rangle \in \mathbb{C}^{2^n}$ and $||\psi_n^k|| = 1$. Fix an n is such that $n^{-1}\sum_{i<n}\mathrm{Tr}(\rho_n P_i^n) > 0.5 + \delta$. We will drop the n subscript of ψ_n^k as the n is fixed. For any $k < 2^n$ we can decompose ψ^k as,

$$\psi^k = c_o^k\psi_o^k + c_p^k\psi_p^k \tag{2.15}$$

where $\psi_o^k \in \mathrm{range}(S_n)$ and $\psi_p^k \in \mathrm{range}(S_n)^{\perp}$ are unit vectors and $c_o^k, c_p^k \in \mathbb{C}$ satisfy $|c_0^k|^2 + |c_p^k|^2 = 1$. We now show that $\dfrac{\delta^2}{36}$ is a lower bound for $\mathrm{Tr}(\rho_n S_n) = \sum_{k<2^n}\alpha_k|c_o^k|^2$.

Note that

$$n^{-1}\sum_{i<n}\mathrm{Tr}(\rho_n P_i^n) \tag{2.16}$$

$$= n^{-1}\sum_{i<n}\sum_{k<2^n}\alpha_k\langle\psi^k|P_i^n|\psi^k\rangle \tag{2.17}$$

$$= \sum_{k<2^n}\alpha_k\big(n^{-1}\sum_{i<n}\langle\psi^k|P_i^n|\psi^k\rangle\big). \tag{2.18}$$

For each fixed k and i, by the same argument as in equation (2.2) and using that $|c_p^k|, |P_i^n\psi_p^k| \leqslant 1$ we have that

$$\langle\psi^k|P_i^n|\psi^k\rangle \leqslant |c_o^k|^2|P_i^n\psi_o^k|^2 + |c_p^k|^2|P_i^n\psi_p^k|^2 + 2|c_o^k||P_i^n\psi_o^k|. \tag{2.19}$$

Using this, we bound the term in parentheses in equation (2.18) for each k. As k is fixed, replace ψ^k and c^k in equation (2.19) by ψ and c respectively for convenience.

$$n^{-1}\sum_{i<n}\langle\psi|P_i^n|\psi\rangle \tag{2.20}$$

$$\leqslant |c_o|^2 n^{-1}\sum_{i<n}|P_i^n\psi_o|^2 + |c_p|^2 n^{-1}\sum_{i<n}|P_i^n\psi_p|^2 + 2|c_o|n^{-1}\sum_{i<n}|P_i^n\psi_o| \tag{2.21}$$

$$\leqslant |c_o| + n^{-1}\sum_{i<n}|P_i^n\psi_p|^2 + 2|c_o| \tag{2.22}$$

$$= n^{-1}\sum_{i<n}|P_i^n\psi_p|^2 + 3|c_o|. \tag{2.23}$$

We used convexity and $|c_p|^2 \leqslant 1, |c_o| \leqslant 1, |P_i^n\psi_o| \leqslant 1$ when obtaining the last inequality. Let $\psi := \psi_p$ and for a fixed $i < n$, let $P := P_i^n$ and consider the summand, $|P\psi|^2$ in the sum in equation (2.23) (we suppressed the indices merely for convenience). Since $\psi \in \mathrm{range}(S_n)^\perp = \mathrm{span}(C_n^c)$, let a_σ be complex numbers such that

$$\sum_{\sigma\notin C_n} a_\sigma^2 = 1,$$

and

$$\psi = \sum_{\sigma \notin C_n} a_\sigma \sigma.$$

Using that $P^* = P$ and $P = P^2$,

$$|P\psi|^2 = \big\langle P\psi | P\psi \big\rangle = \big\langle \psi | P\psi \big\rangle \tag{2.24}$$

$$= \big\langle \sum_{\sigma \notin C_n} a_\sigma \sigma | \sum_{\tau \notin C_n} a_\tau P\tau \big\rangle \tag{2.25}$$

$$= \sum_{\sigma \notin C_n} \sum_{\tau \notin C_n} a^*_\sigma a_\tau \big\langle \sigma | P\tau \big\rangle. \tag{2.26}$$

Note that $P\tau = \tau$ or $P\tau = 0$ and that $\big\langle \sigma | \tau \big\rangle = \delta_{\sigma=\tau}$. So, $\big\langle \sigma | P\tau \big\rangle$ is zero whenever $\sigma \neq \tau$ (Here we used that the orthonormal vectors spanning C_n^c are eigenvectors of P). So, (2.26) becomes,

$$|P\psi|^2 \leqslant \sum_{\sigma \notin C_n} a^2_\sigma \big\langle \sigma | P\sigma \big\rangle.$$

Using this and reinserting the indices, the first term in (2.23) is bounded above by

$$n^{-1} \sum_{i<n} \sum_{\sigma \notin C_n} (a^k_\sigma)^2 \big\langle \sigma | P^n_i \sigma \big\rangle.$$

Finally, putting this back in (2.18),

$$\sum_{k<2^n} \alpha_k \big(n^{-1} \sum_{i<n} \big\langle \psi^k | P^n_i | \psi^k \big\rangle \big) \tag{2.27}$$

$$\leqslant \sum_{k<2^n} \alpha_k \big(n^{-1} \sum_{i<n} \sum_{\sigma \notin C_n} (a^k_\sigma)^2 \big\langle \sigma | P^n_i \sigma \big\rangle + 3|c^k_o| \big) \tag{2.28}$$

$$\leqslant \sum_{k<2^n} \alpha_k \big(\sum_{\sigma \notin C_n} (a^k_\sigma)^2 n^{-1} \sum_{i<n} \big\langle \sigma | P^n_i \sigma \big\rangle \big) + \sum_{k<2^n} \alpha_k 3|c^k_o| \tag{2.29}$$

$$\leqslant \big(\sum_{k<2^n} \alpha_k \sum_{\sigma \notin C_n} (a^k_\sigma)^2 (\delta/2 + 0.5) \big) + 3 \sum_{k<2^n} \alpha_k |c^k_o| \tag{2.30}$$

$$\leqslant (\delta/2 + 0.5) \big(\sum_{k<2^n} \alpha_k \sum_{\sigma \notin C_n} (a^k_\sigma)^2 \big) + 3 \sum_{k<2^n} \alpha_k |c^k_o| \tag{2.31}$$

$$\leqslant (\delta/2 + 0.5) + 3 \sum_{k<2^n} \alpha_k |c^k_o|. \tag{2.32}$$

In getting (2.30) we used the definition of C_n. In the last step we used that $\sum_{\sigma \notin C_n} (a^k_\sigma)^2 = 1$ for all k and convexity. In summary, we have shown that for infinitely many n,

$$0.5 + \delta < n^{-1} \sum_{i<n} \mathrm{Tr}(\rho_n P^n_i) = \sum_{k<2^n} \alpha_k \big(n^{-1} \sum_{i<n} \big\langle \psi^k | P^n_i | \psi^k \big\rangle \big) \leqslant (\delta/2 + 0.5) + 3 \sum_{k<2^n} \alpha_k |c^k_o|.$$

So, by Jensen's inequality

$$\delta^2/36 < \big(\sum_{k<2^n} \alpha_k |c^k_o| \big)^2 \leqslant \sum_{k<2^n} \alpha_k |c^k_o|^2 = \mathrm{Tr}(\rho_n S_n),$$

for infinitely many n. So, ρ fails a quantum Schnorr test at $\delta^2/36$, a contradiciton. Now if $\exists^\infty n$, with $n^{-1} \sum_{i<n} \mathrm{Tr}(\rho_n P^n_i) < -\delta + 0.5$ then define

$$Q^n_i = (P^n_i)^\perp := \sum_{\sigma : |\sigma| = n, \sigma(i) = 0} |\sigma\rangle\langle\sigma|.$$

Note that $\mathrm{Tr}(\rho_n Q^n_i) + \mathrm{Tr}(\rho_n P^n_i) = 1$ for all i, n. So, for infinitely many n, $1 = n^{-1}(\sum_{i<n} \mathrm{Tr}(\rho_n P^n_i) + \sum_{i<n} \mathrm{Tr}(\rho_n Q^n_i)) < -\delta + 0.5 + \mathrm{Tr}(\rho_n Q^n_i))$. I.e, $n^{-1} \sum_{i<n} \mathrm{Tr}(\rho_n Q^n_i) > \delta + 0.5$ for infinitely many n. Now, we can repeat the proof as in case 1 with Q replacing P and 0s replacing the 1s. □

2.5 A Shannon–McMillan–Breiman Theorem for quantum Schnorr randoms

The Shannon–McMillan–Breiman (SMB) theorem for bitstrings roughly says that for an ergodic measure, μ, on Cantor space the empirical entropy for μ almost every trajectory (infinite bitstring) equals the entropy of μ. There have also been effective versions of the SMB. For example, it has been shown that the exception set for the SMB theorem in the

classical setting can be covered by a Martin-Löf test [24]. In the quantum setting, where we do not have a notion of 'almost every', we may replace 'μ almost every trajectory' by 'every μ Schnorr random state' as we do here. A special case of the SMB theorem for infinite sequences of qubits was first studied by Nies and Tomamichel [29]. To formalize a μ Schnorr random state in the quantum setting, we need a definition

Definition 2.29. A computable sequence of special projections is a μ *quantum Schnorr test* if $\sum_{k\in\omega} \mu(S^k)$ is computable.

A state ρ is μ quantum Schnorr random if it passes all μ quantum Schnorr tests. A similar definition for quantum MLR states was made by Nies and Tomamichel [29]. Intuitively, a μ quantum Schnorr random state is a 'trajectory' in the state space [31] which is random in the sense of μ.

Theorem 2.30. Let $\mu = (\mu_n)_n$ be a state of the form $\mu_n = \otimes_1^n M$ for an M of the form

$$\begin{bmatrix} p & 0 \\ 0 & 1-p \end{bmatrix},$$

for some computable $p \in (0,1)$. If ρ is μ quantum Schnorr random, then $\lim_n n^{-1}\mathrm{Tr}(-\rho_n \log(\mu_n)) = h(\mu)$, the von-Neumann entropy of M.

Intuitively, the theorem says that along any μ Schnorr random state, ρ, the empirical entropy, $n^{-1}\mathrm{Tr}(-\rho_n \log(\mu_n))$ limits to the entropy of μ, which equals that of M as μ is a product tensor.

Proof. Let M be as given and first, assume that $p \leqslant 0.5$. We prove it by contradiction. Define $L_n = -\log\mu_n$ for all n and $h := h(\mu)$. Suppose ρ is quantum Schnorr random but there is a δ such that either $\exists^\infty n$, with $n^{-1}\mathrm{Tr}(\rho_n L_n) > \delta + h$ or $\exists^\infty n$, with $n^{-1}\mathrm{Tr}(\rho_n L_n) <$

$-\delta+h$. Suppose first that the former holds. The proof is similar to that of the law of large numbers, but different techniques are needed as L_n is not a projection. σ will always be used to denote classical bitstrings. For σ of length n, $\langle\sigma|\mu_n|\sigma\rangle = \mu(\sigma,\sigma) = p^k(1-p)^{n-k}$ where k = numbers of zeros in σ. So, μ can be thought of a i.i.d. measure on Cantor space assigning $\mu(0) = p, \mu(1) = 1-p$.

Define for all n,

$$C_n = \left\{\sigma : |\sigma| = n, -n^{-1}\log\mu(\sigma) > \delta/2 + h\right\}.$$

Let S_n be the special projection,

$$S_n := \sum_{\sigma\in C_n} |\sigma\rangle\langle\sigma|.$$

$(S_n)_n$ is a computable sequence since we may let δ be rational. By the Chernoff bound, $\mu(S_n) = 2^{-n}|C_n| \leqslant 2\exp(-0.5n\delta^2)$ for all n. So, $\sum_n \mu(S_n)$ is computable showing that $(S_n)_n$ is a $\mu-$quantum Schnorr test.

For all n, let

$$\rho_n = \sum_{k<2^n} \alpha_k |\psi_n^k\rangle\langle\psi_n^k|$$

for α_k non-negative real numbers with $\sum_{k<2^n}\alpha_k = 1$ and for each k, $|\psi_n^k\rangle \in \mathbb{C}^{2^n}$ and $||\psi_n^k|| = 1$. Fix an n is such that $n^{-1}\mathrm{Tr}(\rho_n L_n) > \delta + h$. We will drop the n subscript of ψ_n^k as the n is fixed. For any $k < 2^n$ we can decompose ψ^k as,

$$\psi^k = c_o^k\psi_o^k + c_p^k\psi_p^k \tag{2.33}$$

where $\psi_o^k \in \mathrm{range}(S_n)$ and $\psi_p^k \in \mathrm{range}(S_n)^\perp$ are unit vectors and $c_o^k, c_p^k \in \mathbb{C}$ satisfy

$|c_0^k|^2 + |c_p^k|^2 = 1$. We find a lower bound, for $\mathrm{Tr}(\rho_n S_n) = \sum_{k<2^n} \alpha_k |c_o^k|^2$ independent of n.

$$n^{-1}\mathrm{Tr}(\rho_n L_n) \tag{2.34}$$

$$= n^{-1} \sum_{k<2^n} \alpha_k \langle \psi^k | L_n | \psi^k \rangle \tag{2.35}$$

$$= \sum_{k<2^n} \alpha_k \big(n^{-1} \langle \psi^k | L_n | \psi^k \rangle \big). \tag{2.36}$$

Fix a k and suppress it in the indices (i.e for example, let $\psi = \psi^k$). By Cauchy-Schwarz and by the self-adjointness and positivity of L_n,

$$\begin{aligned}
\langle \psi^k | L_n | \psi^k \rangle &\leqslant |c_o|^2 \langle \psi_o | L_n \psi_o \rangle + |c_p|^2 \langle \psi_p | L_n \psi_p \rangle + 2|c_o||c_p| |\langle \sqrt{L_n}\psi_p | \sqrt{L_n}\psi_o \rangle| \\
&\leqslant |c_o|^2 \langle \psi_o | L_n \psi_o \rangle + |c_p|^2 \langle \psi_p | L_n \psi_p \rangle + 2|c_o| |\sqrt{L_n}\psi_p| |\sqrt{L_n}\psi_o| \\
&\leqslant |c_o|^2 \langle \psi_o | L_n \psi_o \rangle + |c_p|^2 \langle \psi_p | L_n \psi_p \rangle + 2|c_o| (||\sqrt{L_n}||_2)^2,
\end{aligned}$$

where $||\cdot||_2$ denotes the L_2 operator norm. M_n, the maximum element of the set

$$\{-j\log p - (n-j)\log(1-p) : 0 \leqslant j \leqslant n\}$$

is the largest eigenvalue of L_n and so, $\sqrt{M_n}$ is the largest eigenvalue of $\sqrt{L_n}$. Noting that the L_2 norm of a real diagonal matrix is equal to its largest eigenvalue and that the Rayleigh quotient of a Hermitian matrix is bounded above by the largest eigenvalue, we see that

$$\begin{aligned}
\langle \psi^k | L_n | \psi^k \rangle &\leqslant |c_o|^2 \langle \psi_o | L_n \psi_o \rangle + |c_p|^2 \langle \psi_p | L_n \psi_p \rangle + 2|c_o| \sqrt{M_n}^2 \\
&\leqslant |c_o|^2 M_n + |c_p|^2 \langle \psi_p | L_n \psi_p \rangle + 2|c_o| M_n \\
&\leqslant 3|c_o| M_n + |c_p|^2 \langle \psi_p | L_n \psi_p \rangle.
\end{aligned}$$

By this and noting that $n^{-1}M_n \leqslant \theta =$ the maximum of $-\log(p)$ and $-\log(1-p)$, we get an upper bound for the term in parentheses in equation (2.36) for each k:

$$n^{-1}\langle \psi^k | L_n | \psi^k \rangle \leqslant 3|c_o^k|\theta + n^{-1}\langle \psi_p^k | L_n \psi_p^k \rangle. \tag{2.37}$$

Since $\psi_p^k \in \text{range}(S_n)^\perp = \text{span}(C_n^c)$, there are a_σs such that

$$\sum_{\sigma \notin C_n} a_\sigma^2 = 1,$$

and

$$\psi_p^k = \sum_{\sigma \notin C_n} a_\sigma^k \sigma.$$

Letting $\psi = \psi_p^k$ and dropping the k indices for convenience.

$$n^{-1}\langle \psi | L_n \psi \rangle \tag{2.38}$$

$$= n^{-1}\langle \sum_{\sigma \notin C_n} a_\sigma \sigma | \sum_{\tau \notin C_n} a_\tau L_n \tau \rangle \tag{2.39}$$

$$= n^{-1} \sum_{\sigma \notin C_n} \sum_{\tau \notin C_n} a_\sigma^* a_\tau \langle \sigma | L_n \tau \rangle. \tag{2.40}$$

As L_n is diagonal and C_n is composed of classical bitstrings, equation (2.40) becomes,

$$\leqslant \sum_{\sigma \notin C_n} |a_\sigma|^2 n^{-1}\langle \sigma | L_n \sigma \rangle = -\sum_{\sigma \notin C_n} |a_\sigma|^2 n^{-1} \log\mu(\sigma)$$

$$\leqslant \sum_{\sigma \notin C_n} |a_\sigma|^2 (\delta/2 + h) \leqslant \delta/2 + h.$$

We used here that the σth entry along the diagonal of L_n is $-\log\mu(\sigma) = -k\log p - (n-k)\log(1-p)$ where $k =$ number of zeros in σ and the definition of C_n. This and (2.37) gives that,

$$n^{-1}\langle \psi^k | L_n | \psi^k \rangle \leqslant 3|c_o^k|\theta + \delta/2 + h. \tag{2.41}$$

Finally, putting this back in (2.36),

$$\sum_{k<2^n} \alpha_k \big(n^{-1}\langle \psi^k | L_n | \psi^k \rangle\big) \leqslant \sum_{k<2^n} \alpha_k \big(3|c_o^k|\theta + \delta/2 + h\big) \leqslant (\delta/2 + h) + 3\theta \sum_{k<2^n} \alpha_k |c_o^k|.$$

In summary, we have shown that for infinitely many n,

$$h + \delta < n^{-1} \sum_{i<n} \mathrm{Tr}(\rho_n P_i^n) \leqslant (\delta/2 + h) + 3\theta \sum_{k<2^n} \alpha_k |c_o^k|.$$

So, by Jensen's inequality

$$\delta^2/36\theta^2 < \big(\sum_{k<2^n} \alpha_k |c_o^k| \big)^2 \leqslant \sum_{k<2^n} \alpha_k |c_o^k|^2 = \mathrm{Tr}(\rho_n S_n),$$

for infinitely many n. So, ρ fails a $\mu-$quantum Schnorr test; a contradiciton. We need to now consider the other case: $\exists^\infty n$, with $n^{-1}\mathrm{Tr}(\rho_n L_n) < -\delta + h$. Define M' to be the reflection of M. I.e., M' is

$$\begin{bmatrix} 1-p & 0 \\ 0 & p \end{bmatrix},$$

and μ' is the i.i.d. measure on Cantor space given by M'. Let $L_n' := -\log \otimes_1^n M'$. Note that for σ of length n, $\langle \sigma | \otimes_1^n M' | \sigma \rangle = p^{n-k}(1-p)^k$ where $k =$ numbers of zeros in σ. Letting $Q_n := L_n + L_n'$, for any length n string σ having k many zeros,

$$\langle \sigma | Q_n | \sigma \rangle = -(n-k)\log(1-p) - k\log(p) - (n-k)\log(p) - k\log(1-p) = -n(\log(p) + \log(1-p)).$$

So, $Q_n = -n(\log(p) + \log(1-p))I_{2^n}$.

$$n^{-1}\mathrm{Tr}(\rho_n L_n) + n^{-1}\mathrm{Tr}(\rho_n L_n') = n^{-1}\mathrm{Tr}(\rho_n Q_n) = -\log(p) - \log(1-p). \tag{2.42}$$

We see that,

$$\begin{aligned} & 2h \leqslant -\log(p) - \log(1-p) \\ & \iff 2p\log(p) + 2(1-p)\log(1-p) \geqslant \log(p) + \log(1-p) \\ & \iff \log(1-p) \geqslant \log(p) \iff p \leqslant 0.5. \end{aligned}$$

(We used here that $p \leqslant 0.5$ and hence that $(1-2p) \geqslant 0$.) So, for one of the infinitely many n such that, $n^{-1}\mathrm{Tr}(\rho_n L_n) < -\delta + h$, equation (2.42) gives that

$$\begin{aligned} & (-\delta + h) + n^{-1}\mathrm{Tr}(\rho_n L_n^{'}) \\ & > n^{-1}\mathrm{Tr}(\rho_n L_n) + n^{-1}\mathrm{Tr}(\rho_n L_n^{'}) = -\log(1-p) - \log(p) \geqslant 2h. \end{aligned}$$

So, there are infinitely many ns with

$$n^{-1}\mathrm{Tr}(\rho_n L_n^{'}) > \delta + h.$$

Since M' has the same entropy as M, we can repeat the proof of the former case using $L_n^{'}, \mu^{'}$ instead of L_n, μ respectively. This completes the proof for $p \leqslant 0.5$. If $p > 0.5$, then repeat the proof for $p \leqslant 0.5$ with $1 - p \leqslant 0.5$ replacing p [The first case has the same proof as it does not depend on the value of p. When proving the second case, M' is $\mathrm{diag}(p, 1-p)$ and the proof goes through since $1 - p \leqslant 0.5$.] $\square$

Chapter 3

Prefix-free quantum Kolmogorov Complexity

3.1 Introduction

The results in this chapter have been published already in the literature [10]. With the intent of developing a quantum version of K, we introduce QK, a notion of descriptive complexity for density matrices using classical prefix-free Turing machines. Many connections between K and Solovay and Schnorr randomness in the classical theory turn out to have analogous connections connections between QK and weak Solovay and quantum Schnorr randomness.

To the best of our knowledge, the current work is the only one to study the incompressibility of initial segments (in the sense of prefix-free classical Turing machines) of weak Solovay and quantum Schnorr random states. Nies and Scholz have explored connections between quantum Martin-Löf randomness and a version of QC using unitary (quantum) machines [31]. We give an overview of the main points in this chapter.

In Section 3.2 we introduce quantum-K (QK) for density matrices and some of its properties. Theorem 3.2 (generalized in Lemma 3.6) shows that QK agrees with K on the classical qubitstrings. Theorem 3.7 is a tight upper bound for QK similar to that for

K. Theorem 3.10 is a counting condition similar to that for QC [8], C and K [21, 28].

Section 3.3, the main focus of this chapter, connects QK with two quantum algorithmic randomness notions: weak Solovay randomness and quantum Schnorr randomness. Two important characterizations show that the initial segments of Martin-Löf randoms (equivalently, of Solovay randoms) are asymptotically incompressible in the sense of K: the Chaitin characterization (See [16] and theorem 3.2.21 in [28]),

$$X \text{ is Martin-Löf random } \iff \lim_n K(X \upharpoonright n) - n = \infty,$$

and the Levin–Schnorr characterization (See theorem 3.2.9 in [28]),

$$X \text{ is Martin-Löf random } \iff \exists c \forall n [K(X \upharpoonright n) > n - c].$$

(Characterizations having the former form will be called 'Chaitin type' and those having the latter form will be called 'Levin–Schnorr type'). We investigate the extent to which these classical characterizations carry over to weak Solovay randoms and QK.

Theorem 3.11 is a Chaitin type of characterization of weak Solovay randomness (ρ is weak Solovay random $\iff \lim_n QK^\epsilon(\rho_n) - n = \infty$). This shows that the Levin–Schnorr condition ($\forall n [QK^\epsilon(\rho_n) >^+ n]$) is implied by weak Solovay randomness.

Theorem 3.13 shows both Chaitin and Levin–Schnorr type characterizations of weak Solovay randomness when restricting attention to a specific class of states. It is worth noting that Theorem 3.13 uses the proof of our main result (Theorem 2.11) in [11].

For general states, subsection 3.3.3 shows that the Levin–Schnorr condition implies something slightly weaker than weak Solovay randomness.

While K plays well with Solovay randomness, K_C, a version of K using a computable measure machine, C (a prefix-free Turing machine whose domain has computable

Lebesgue measure) gives a Levin–Schnorr characterization of Schnorr randomness (See theorem 7.1.15 in [21]). Motivated by this, we introduce QK_C a version of QK using computable measure machines in subsection 3.3.4.

It turns out that QK_C yields not just a Levin–Schnorr type (Theorem 3.22), but also a Chaitin type (Theorem 3.23) characterization of quantum Schnorr randomness.

Theorem 3.23 together with Theorem 3.20 and lemma 3.9 in [11], implies that Schnorr randoms have a Chaitin type characterization in terms of K_C (Theorem 3.24). So, results in the quantum realm imply a new result in the classical setting.

In summary, we introduce QK and show that the initial segments of weak Solovay random and quantum Schnorr random states are incompressible in the sense of QK.

3.2 The Definition and Properties of QK

We assume familiarity with the notions of density matrix (See for example, [27]), prefix-free Kolmogorov complexity (K) and $\mathbb{U}$, the universal prefix-free (or self-delimiting) Turing machine (See [14, 21, 28]).

The output of $\mathbb{U}$ can be interpreted as unordered tuples of complex algebraic vectors (equivalently, finite subsets of natural numbers).

The notation $\mathbb{U}(\sigma) \downarrow = F$ means that $\mathbb{U}(\sigma)$ outputs the index of F with respect to some fixed canonical indexing of finite subsets of the naturals. We will never use an ordering on the elements of F in any of our arguments: F will be used to define an orthogonal projection : $\sum_{v \in F} |v\rangle\langle v|$ which clearly does not depend on an ordering on F.

As explained in [31], the quantum analogue of a bitstring of length n is a density matrix on $\mathbb{C}^{2^n}$.

For a density matrix, τ, let $|\tau|$ denote the s such that τ is a transformation on $\mathbb{C}^{2^s}$. For any n, $\mathbb{C}^{2^n}_{alg}$ is the space of elements of $\mathbb{C}^{2^n}$ with complex algebraic entries.

Logarithms will always be base 2. The notation $\leqslant^+, \geqslant^+, =^+$ will be used for 'upto additive constant' relations.

For $\epsilon > 0$, $QK^\epsilon(\tau)$ is defined to be

Definition 3.1. $QK^\epsilon(\tau) := \inf\{|\sigma| + \log|F| : \mathbb{U}(\sigma) \downarrow = F$, a orthonormal set in $\mathbb{C}^{2^{|\tau|}}_{alg}$ and $\sum_{v\in F} \langle v|\tau|v\rangle > \epsilon\}$

The term $\sum_{v\in F} \langle v|\tau|v\rangle$ is the squared length of the 'projection of τ onto span(F)' which also equals the probability of getting an outcome of '1' when measuring τ with the observable given by the Hermitian projection onto span(F) [27]. Although it is useful to intuitively think of $\sum_{v\in F} \langle v|\tau|v\rangle$ as the 'projection of τ onto span(F)', we use quotes as τ is a convex combination of possibly *multiple* unit vectors, while the notion 'projection onto a subspace' refers usually to a single vector.

Note that for a given τ, $QK^\epsilon(\tau)$ is determined by the classical prefix-free complexities and dimensions of those subspaces, span(F), such that the projection of τ onto span(F) has squared length atleast ϵ. I.e., $QK^\epsilon(\tau)$ depends only on the K-complexities and ranks of those projective measurements of τ such that the probability of getting an outcome of '1' is atleast ϵ. Roughly speaking, $QK^\epsilon(\tau)$ depends on the dimensions and prefix-free complexities of subspaces which are ϵ 'close' to τ.

This is in contrast to $QC^\epsilon(\tau)$ which depends on the quantum complexities of density matrices, not classical prefix-free complexities of subspaces, which are ϵ close to τ (Recall that QC is based on quantum Turing machines) [8]. Also, while the rank of the approximating projection is taken into consideration in QK, the rank of the approximating

density matrix is not taken into account in QC.

So, $QC^{\epsilon}(\tau)$ quantifies the quantum complexity of approximating τ by density matrices upto ϵ while $QK^{\epsilon}(\tau)$ measures the sum of the prefix-free complexity and the logarithm of the dimension of subspaces ϵ close to τ.

A test demonstrating the quantum non-randomness of a state, ρ uses computable sequences of projections of 'small rank' which are ϵ-close to initial segments (density matrices) of ρ. It hence seems plausible that a complexity measure for a density matrix, τ must reflect the complexities and ranks of projections ϵ-close to τ in order to play well with quantum randomness notions for states.

We mention that our QK is entirely different from the $\overline{QK_M}$ and $\overline{QK_M^{\delta}}$ notions defined in Definition 3.1.1 in [26] using quantum Turing machines.

QK^{ϵ} would not be a 'natural' complexity notion for density matrices if the following theorem did not hold:

Theorem 3.2. Fix a rational ϵ. $K(\sigma) = QK^{\epsilon}(|\sigma\rangle\langle\sigma|)$ holds for all classical bitstrings σ, upto an additive constant depending only on ϵ.

We isolate here a simple but useful property which will be used for proving Theorem 3.2.

Lemma 3.3. Let n be a natural number, $E = (e_i)_{i=1}^{2^n}$ be any orthonormal basis for $\mathbb{C}^{2^n}$ and F be any Hermitian projection matrix acting on $\mathbb{C}^{2^n}$. For any $\delta > 0$, let

$$S_{E,F}^{\delta} := \{e_i \in E : \langle e_i|F|e_i\rangle > \delta\}.$$

Then, $|S_{E,F}^{\delta}| < \delta^{-1}\mathrm{Tr}(F)$.

Proof. Note that since F is a Hermitian projection, $\langle e_i|F|e_i\rangle = \langle Fe_i|Fe_i\rangle = |Fe_i|^2 \geqslant 0$. So,

$$\delta|S^{\delta}_{E,F}| < \sum_{e_i \in S^{\delta}_{E,F}} \langle e_i|F|e_i\rangle \leqslant \sum_{i \leqslant 2^n} \langle e_i|F|e_i\rangle = \mathrm{Tr}(F).$$

□

Proof. We now prove Theorem 3.2, the idea of which is as follows: Given a classical bitstring and a subspace 'close' to it, we find a subspace spanned only by classical bitstrings 'close' to this subspace. Then we compress each of the spanning classical strings and show that the string we began with must be one of these. Fix a rational ϵ. Consider the machine P doing the following:

1. On input π, P searches for $\pi = \sigma\tau$ such that $\mathbb{U}(\sigma) \downarrow = F$, an orthonormal set, $F \subseteq \mathbb{C}^{2^n}_{alg}$ for some n and $|\tau| = \lceil \log(\epsilon^{-1}|F|)\rceil$.

2. Letting $O := \sum_{v \in F} |v\rangle\langle v|$ and E, the standard basis of $\mathbb{C}^{2^n}$, find the set $S^{\epsilon}_{E,O}$ from Lemma 3.3.

3. Take a canonical surjective map g from the set of bitstrings of length $\lceil \log(\epsilon^{-1}|F|)\rceil$ onto $S^{\epsilon}_{E,O}$. (g exists since $|S^{\epsilon}_{E,O}| < \epsilon^{-1}|F|$ by 3.3). Output $g(\tau)$.

We first show that P is prefix-free. Suppose π and π' are in the domain of P and $\pi \preceq \pi'$. Then, $\pi = \sigma\tau$ and $\pi' = \sigma'\tau'$ and σ and σ' are in the domain of $\mathbb{U}$. $\pi \preceq \pi'$ implies that $\sigma \preceq \sigma'$ or $\sigma' \preceq \sigma$. But as $\mathbb{U}$ is prefix-free, $\sigma = \sigma'$ must hold. Since the computations $\mathbb{U}(\pi)$, and $\mathbb{U}(\pi')$ and not stuck forever at (1), it must be that $|\tau| = \lceil \log(\epsilon^{-1}|F|)\rceil$ and $|\tau'| = \lceil \log(\epsilon^{-1}|F'|)\rceil$ where $\mathbb{U}(\sigma) \downarrow = F = F' = \mathbb{U}(\sigma') \downarrow$. So, τ and τ' have the same length implying that $\pi = \pi'$.

Now, let $\sigma \in 2^n$ be any classical bitstring. Let λ and $F \subseteq \mathbb{C}^{2^n}_{alg}$ a orthonormal set

such that $|\lambda| + \log(|F|) = QK^{\epsilon}(|\sigma\rangle\langle\sigma|)$, $\sum_{v\in F} \langle v|\sigma\rangle\langle\sigma|v\rangle > \epsilon$ and $\mathbb{U}(\lambda) = F$. Let $O := \sum_{v\in F} |v\rangle\langle v|$. Note that since $\epsilon < \sum_{v\in F} \langle v|\sigma\rangle\langle\sigma|v\rangle = \langle\sigma|O|\sigma\rangle$, $\sigma \in S^{\epsilon}_{E,O}$ where E is the standard basis. Let τ be a length $\lceil \log(\epsilon^{-1}|F|)\rceil$ string such that $g(\tau) = \sigma$. Then, we see that $P(\lambda\tau) = \sigma$.

$$\mathrm{K}(\sigma) \leqslant^{+} |\lambda| + |\tau| \leqslant^{+} |\lambda| + \log(\epsilon^{-1}) + \log(|F|) \leqslant^{+} QK^{\epsilon}(|\sigma\rangle\langle\sigma|)$$

This establishes one direction. Note that the additive constant depends on ϵ. The constant (zero) in the other direction turns out to be independent of ϵ: Given some classical bitstring σ, let $\mathbb{U}(\pi) = \sigma$ and $|\pi| = \mathrm{K}(\sigma)$. Then, letting $F = \{\sigma\}$ in 3.19, $QK^{\epsilon}(\sigma) \leqslant QK^{1}(\sigma) \leqslant |\pi| = K(\sigma)$, for any $\epsilon > 0$.

□

Definition 3.4. A 'system' $B = ((b^n_0, b^n_1))_{n\in\mathbb{N}}$ is a sequence of orthonormal bases for $\mathbb{C}^2$ such that each b^n_i is complex algebraic and the sequence $((b^n_0, b^n_1))_{n\in\mathbb{N}}$ is computable.

Remark 3.5. Let $B = ((b^n_0, b^n_1))_{n\in\mathbb{N}}$ be a system, as in 4.2. Let A_B be the set of all pure states, σ such that σ is a product tensor of elements from B. For example, $b^1_0 \otimes b^2_1 \otimes b^3_1 \otimes b^4_0 \in A_B$. Then, the previous theorem generalizes to the following: Fix a rational ϵ, a B and a A_B as above. $K(\sigma) =^{+} QK^{\epsilon}(|\sigma\rangle\langle\sigma|)$ holds for all $\sigma \in A_B$, upto an additive constant depending only on B and ϵ. Here, $K(\sigma)$ is defined in the obvious way. For example, $K(b^1_0 \otimes b^2_1 \otimes b^3_1 \otimes b^4_0) = K(0110)$. This is proved by replacing $S^{\epsilon}_{E,O}$ with $S^{\epsilon}_{B,O}$ in the proof of Theorem 3.2.

The following lemma can be proved similarly to Theorem 3.2.

Lemma 3.6. Fix a rational ϵ and let $(B_n)_n$ be a computable sequence such that B_n is a orthonormal basis for $\mathbb{C}^{2^n}$ composed of algebraic complex vectors. Then, for all

$\sigma \in \bigcup_n B_n$, $K(\sigma) = QK^{\epsilon}(|\sigma\rangle\langle\sigma|)$, upto an additive constant depending only on ϵ and $(B_n)_n$.

Note that $K(\sigma)$ is well-defined as σ is complex algebraic. The following Theorem 3.7 agrees nicely with the upper bound for K in the classical setting: for all strings x, $K(x) \leqslant |x| + K(|x|) + 1$ (See theorem 2.2.9 in [28].).

Theorem 3.7. There is a constant $d > 0$ such that for any ϵ and any τ, $\mathrm{QK}^{\epsilon}(\tau) \leqslant |\tau| + \mathrm{K}(|\tau|) + d$.

Proof. Let $k > 1$. Let P be the prefix-free Turing machine which on input π, such that $\mathbb{U}(\pi) = n$ outputs $E = (e_i)_{i=1}^{2^n}$, the standard computational basis of $\mathbb{C}^{2^n}$. □

It may seem that this upper bound, given by the apparently inefficient device of using $2^{|\tau|}$ many orthonormal vectors to approximate τ, can be improved. However, the bound is tight by Theorem 3.2 together with the classical counting theorem (see [21], theorem 3.7.6.).

As we shall see later, the unique tracial state $\tau = (\tau_n)_{n\in\mathbb{N}}$ where for all n, τ_n is the 2^n by 2^n diagonal matrix with 2^{-n} along the diagonal is quantum Martin-Löf random. Theorem 3.8 shows that its initial segments achieve the upper bound given by Theorem 3.7.

Theorem 3.8. Let k be any natural number. There is a constant t such that for all n, $QK^{2^{-k}}(\tau_n) \geqslant n + K(n) - t$.

Proof. Fix a k and suppose towards a contradiction that for all $t \in \mathbb{N}$, there is a n_t such that $QK^{2^{-k}}(\tau_{n_t}) < n_t + K(n_t) - t$. So, for all t, there are $F_t \subseteq \mathbb{C}^{2^{n_t}}$ and σ_t such that $\mathbb{U}(\sigma_t) = F_t$ and

$$2^{-k} < \sum_{v \in F_t} \langle v|\tau_{n_t}|v\rangle = 2^{-n_t}|F_t|,$$

and

$$|\sigma_t| + \log(|F_t|) < n_t + K(n_t) - t.$$

Taking log on both sides of the first inequality and inserting in the second gives that for all t, n_t and σ_t,

$$t - k + |\sigma_t| < K(n_t). \tag{3.1}$$

Now, define a prefix-free machine M as follows. On input π, M checks if $\mathbb{U}(\pi)$ halts and outputs a orthonormal set $F \subseteq \mathbb{C}^{2^n}$ for some n. If so, then $M(\pi) = n$. Let r be the coding constant of M. Note that for all t, $M(\sigma_t) = n_t$. So, $K(n_t) \leqslant |\sigma_t| + r$. Together with (3.1), we have that for all t, $t - k + |\sigma_t| < |\sigma_t| + r$. So, $t - k < r$ for all t, a contradiction.

□

In contrast to Lemma 3.6, we have,

Lemma 3.9. Fix an $\epsilon > 0$ and an $n \in \mathbb{N}$. It is not true that for all σ, complex algebraic pure states in $\mathbb{C}^{2^n}$, $QK^{\epsilon}(|\sigma\rangle\langle\sigma|) =^{+} K(\sigma)$.

Proof. Clearly, for all σ, complex algebraic pure states, $QK^{\epsilon}(|\sigma\rangle\langle\sigma|) \leqslant^{+} K(\sigma)$ holds. Suppose that for some ϵ and $n \in \mathbb{N}$, for all $\sigma \in \mathbb{C}^{2^n}_{alg}$, pure states, $QK^{\epsilon}(|\sigma\rangle\langle\sigma|) \geqslant^{+} K(\sigma)$ holds. By Theorem 3.7, for all $\sigma \in \mathbb{C}^{2^n}_{alg}$, pure, $K(n) + n \geqslant^{+} QK^{\epsilon}(|\sigma\rangle\langle\sigma|) \geqslant^{+} K(\sigma)$. This is a contradiction as there are only finitely many programs of length atmost $n + K(n)$ but there are infinitely many complex algebraic pure states, σ of length n. □

Analogously to QC [6,8] a 'counting condition' also holds for QK: the cardinality of a orthonormal set of vectors with bounded complexity has an upper bound depending on the complexity bound. The counting condition for QK is established in a different fashion than that for QC (which uses entropy inequalities like Holevo's-chi [8] and Fanne's inequality [6]). This reflects once again that QC invloves approximating a density matrix by another density matrix while QK involves 'projecting' a density matrix onto a subspace.

Theorem 3.10. Let $V = (v_i)_{i=1}^N \subset \mathbb{C}^{2^s}$ be a collection of orthonormal vectors with $QK^\epsilon(|v_i\rangle\langle v_i|) \leqslant B$ for all i. Then, $N \leqslant \epsilon^{-1}2^B$.

Proof. For each v_i, we have σ_i and F_i,

$$F_i = \sum_{t \in A_i} |t\rangle\langle t|,$$

with $A_i \subset \mathbb{C}^{2^s}$ orthonormal, such that $\langle v_i|F_i|v_i\rangle > \epsilon$, $\mathbb{U}(\sigma_i) = F_i$ and $|\sigma_i|+\log|A_i| \leqslant B$. Let $D \subseteq \{1, 2 \cdots N\}$ be maximal such that $F_i \neq F_j$ for i, j in D. ($D \neq \{1, 2 \cdots N\}$ may hold as there may be i, j with $F_i = F_j$). Let F be the orthogonal projector onto the subspace spanned by $A := \bigcup_{i \in D} A_i$. Then, A has dimension atmost $\sum_{i \in D} |A_i|$. By $|A_i| \leqslant 2^{-|\sigma_i|}2^B$ for all i and noting that $\sigma_i \neq \sigma_j$ for i, j in D,

$$\mathrm{Tr}(F) \leqslant \sum_{i \in D} |A_i| \leqslant \sum_{i \in D} 2^{-|\sigma_i|}2^B \leqslant 2^B \sum_{\sigma \in \mathrm{dom}(\mathbb{U})} 2^{-|\sigma|} \leqslant 2^B.$$

The reason behind summing over $i \in D$, rather than over $i \leqslant N$ was to get the second to last inequality. By the maximality of D, $A = \bigcup_{i \leqslant N} A_i$ and so, A_i is a subspace of A for all $i \leqslant N$. So, $\langle v_i|F|v_i\rangle \geqslant \langle v_i|F_i|v_i\rangle > \epsilon$ for all $i \leqslant N$. By orthonormality of V,

$$\epsilon N < \sum_i \langle v_i|F|v_i\rangle \leqslant \mathrm{Tr}(F).$$

□

3.3 Relating QK to randomness

3.3.1 A Chaitin type result

Theorem 3.11 is a Chaitin type characterization of the weak Solovay random states in terms of QK. (Chaitin's result in the classical setting says that an infinite bitstring X is Solovay random if and only $\lim_n K(X \upharpoonright n) - n = \infty$).

Theorem 3.11. A state $\rho = (\rho_n)_n$ is weak Solovay random if and only if

$$\forall \epsilon > 0 \forall c > 0 \forall^\infty n QK^\epsilon(\rho_n) \geqslant n + c.$$

Proof. ($\Longleftarrow$): Suppose for a contradiction that ρ fails a strong Solovay test $(S_m)_m$ at $\epsilon > 0$. The idea will be to use the subspaces given by the S_ms, to approximate ρ. More, precisely, the F appearing in the definition of QK^ϵ will be the orthonormal vectors given by the projection S_m for an appropriate m. The details are as follows. Let M be the prefix-free machine doing the following. On input σ, if $\mathbb{U}(\sigma) = m$, then output $(v_i)_i$ where

$$S_m = \sum_i |v_i\rangle\langle v_i|.$$

Let c_M be it's coding constant. Take an m such that $\mathrm{Tr}(\rho_{n_m} S_m) > \epsilon$ (Notation: n_m is the natural number n such that S_m is a projection on n qubits.). By the choice of m,

$$\mathrm{QK}^\epsilon(\rho_{n_m}) \leqslant \mathrm{K}(m) + c_M + \log(2^{n_m}\tau(S_m)) = n_m + \mathrm{K}(m) - f(m) + c_M,$$

where f is the function: $f(m) = -\log(\tau(S_m))$. As f is computable and as $\sum_m 2^{-f(m)} < \infty$ by the definition of a strong Solovay test, Lemma 3.12.2 in [21] implies that for all m,

$\mathrm{K}(m) - f(m) \leqslant q$ for some constant q. Noting that we may assume the sequence n_m to be strictly increasing in m and letting $c := q + c_M + 1$, we see that $\exists^\infty n$ such that $\mathrm{QK}^\epsilon(\rho_n) < n + c$.

($\Longrightarrow$): Suppose toward a contradiction that there is a $\epsilon > 0$ and a constant $c > 0$ such that there are infinitely many n with $\mathrm{QK}^\epsilon(\rho_n) < n + c$. Define a strong Solovay test S as follows. Let T be the set of all σ such that $\mathbb{U}(\sigma)$ halts and outputs an orthonormal set $F_\sigma \subseteq \mathbb{C}^{2^{n_\sigma}}$ such that $|\sigma| + \log |F_\sigma| < n_\sigma + c$. For all $\sigma \in T$, let

$$P_\sigma := \sum_{v \in F_\sigma} |v\rangle\langle v|$$

and let $S := (P_\sigma)_{\sigma \in T}$. For all $\sigma \in T$, $2^{|\sigma|}|F_\sigma| < 2^{n_\sigma + c}$. So, $\tau(P_\sigma) = 2^{-n_\sigma}|F_\sigma| < 2^{c - |\sigma|}$. So,

$$\sum_{\sigma \in T} \tau(P_\sigma) < 2^c \sum_{\sigma \in T} 2^{-|\sigma|} < 2^c \sum_{\sigma : \mathbb{U}(\sigma)\downarrow} 2^{-|\sigma|} < \infty,$$

since $\mathbb{U}$ is prefix-free. This shows that S is a strong Solovay test. For any n such that $\mathrm{QK}^\epsilon(\rho_n) < n + c$, there is a $\sigma \in T$ such that $\mathrm{Tr}(P_\sigma \rho_n) > \epsilon$. So, ρ fails S at ϵ. □

The following corollary shows the equivalence of weak Solovay and q-ML randomness for a specific type of states. Let $B = ((b_0^n, b_1^n))_{n \in \mathbb{N}}$ be a system (Definition 4.2). Let A_B^∞ be the set of all states which are limits of elements from A_B as in 3.5. For example, $b_0^1 \otimes b_1^2 \otimes b_0^3 \otimes b_1^4 \cdots =: \rho \in A_B^\infty$.

Corollary 3.12. For any B, weak Solovay randomness is equivalent to q-MLR on A_B^∞.

Proof. Fix a system $B = ((b_0^n, b_1^n))_{n \in \mathbb{N}}$ and let $\rho \in A_B^\infty$ be weak Solovay random. Let ρ' be the bitstring induced by ρ. I.e., for example if $\rho = b_0^1 \otimes b_1^2 \otimes b_0^3 \otimes b_1^4 \cdots$, then $\rho' := 0101 \cdots$. By Theorem 3.11, for $\epsilon = 0.5$

$$\forall c > 0 \forall^\infty n QK^{0.5}(\rho_n) \geqslant n + c.$$

By Remark 3.5, $K(\rho' \upharpoonright n) = MK^{0.5}(\rho_n)$ upto a constant depending only on B. So,

$$\forall c > 0 \forall^{\infty} n K(\rho' \upharpoonright n) \geqslant n + c.$$

By Chaitin's result, [16] ρ' is MLR. Now, by an easy modification of 3.13 from [31], ρ is q-MLR. We already know that q-MLR implies weak Solovay randomness for any state from before. □

3.3.2 Chaitin and Levin–Schnorr type results

It turns out that weak Solovay randomness is equivalent to q-MLR and has both Chaitin ((3) in Theorem 3.13) and Levin–Schnorr ((4) in Theorem 3.13) type characterizations in terms of QK when the states are restricted to a certain class, $\mathcal{L}$ defined below. To define this class we need to consider the halting set over the halting set : $\varnothing'' = (\varnothing')'$ (See [28]). Let $\mathcal{L}$ denote the union of the two classes of states.

1. States in A_B^{∞} for some B, as in Corollary 3.12
2. States which do not Turing compute $\varnothing''$.

Nies and Barmpalias (in personal communication) have shown that q-MLR is equivalent to weak quantum Solovay randomness for states which do not compute $\varnothing''$. The same equivalence also holds on A_B^{∞} by Corollary 3.12. This similarity motivates our study of $\mathcal{L}$.

Theorem 3.13. If $\rho = (\rho_n)_n \in \mathcal{L}$, then the following are equivalent

1. ρ is q-MLR.
2. ρ is weak Solovay random.

3. $\forall \epsilon > 0 \forall c > 0 \forall^{\infty} n, QK^{\epsilon}(\rho_n) \geqslant n + c.$

4. $\forall \epsilon > 0 \exists c \forall n, QK^{\epsilon}(\rho_n) > n - c.$

Proof. (1) $\iff$ (2) follows from the previous remarks.

(4)$\Longrightarrow$(1):

Proof. First, let $\rho \in A_B^{\infty}$ for some B and let (4) hold. By the same argument as in Corollary 3.12, we get that

$$\exists c > 0 \forall n, K(\rho' \upharpoonright n) \geqslant n - c.$$

The classical Levin–Schnorr result [21] implies that ρ' is MLR. Using once more 3.13 in [31] as in 3.12, we see that ρ is q-MLR. Now suppose ρ does not Turing compute $\varnothing''$. We will show that (4) implies (2). Suppose for a contradiction that $(S^m)_m$ is a strong Solovay test which ρ fails at $\epsilon' > 0$. By Theorem 2.11 in [11], we can effectively compute a q-MLT $(G^m)_m$ which ρ fails at some rational $\epsilon > 0$. Let $g(m) :=$ the least s such that $\mathrm{Tr}(\rho_s G_s^{2m}) > \epsilon$. As ρ computes g, by Martin's high domination theorem (see [21] for a proof), there is a total computable function f such that $\exists^{\infty} g(n) < f(n)$. We may assume that $f(t) > 3t$ for all t by taking the max of 2 computable functions. Fix this f (non-uniformly) and consider the following machine, M:

On input $0^m 1$, M outputs F^m where F^m is such that

$$G_{f(m)}^{2m} = \sum_{v \in F^m} |v\rangle\langle v|.$$

Clearly M is prefix free. Let $l - 1$ be it's coding constant. Let t be so that $f(t) > g(t)$. Let F^t be defined similarly to F^m above. Then, by definition of g, we have that

$$\epsilon < \sum_{v \in F^t} \langle v|\rho_{f(t)}|v\rangle.$$

$M(0^t1) = F^t$ and so, there is a π such that $|\pi| \leqslant t + l$ and $\mathbb{U}(\pi) = F^t$. Also note that $|F^t| \leqslant 2^{f(t)-2t}$ by the definition of a q-MLT. So, $\mathrm{QK}^\epsilon(\rho_{f(t)}) \leqslant t+l+f(t)-2t = f(t)-t+l$.

Recall that t was an arbitrary element of the infinite set $\{s : f(s) > g(s)\}$. So, for infinitely many ts, there is an $n = f(t)$ such that $\mathrm{QK}^\epsilon(\rho_n) \leqslant n - t + l$, contradicting (4). □

(3) $\Longrightarrow$ (4) is obvious and (2) $\Longrightarrow$ (3) was done in Theorem 3.11. □

We apply the preceding theorem to get the following quantum analog of a classical result, Proposition 3.2.14 in [28].

Theorem 3.14. Let C be an infinite computable set, $\rho \in \mathcal{L}$ and $\epsilon > 0$. If there is a d such that for all $m \in C$, $QK^\epsilon(\rho_m) > m - d$, then ρ is weak Solovay random.

Proof. Let M be the machine doing the following: On input σ, check if $\mathbb{U}(\sigma) = F$, an orthonormal set $F \subseteq \mathbb{C}^{2^n}$. If such a F and n exist, compute s such that $n + s$ is the least element of C greater than n and output the set:

$$T := \{v \otimes \pi : v \in F, \pi \in 2^s\}.$$

Note that $|T| = 2^s|F|$. It is easy to see that M is prefix-free. Let l be it's coding constant. Suppose for a contradiction that ρ is not weak Solovay random. 3.13 implies that $\forall c$, $\exists n_c$ such that $QK^\epsilon(\rho_{n_c}) \leqslant n_c - c$. Let c be arbitrary and take such an $n := n_c$. There is a σ and F such that $\mathbb{U}(\sigma) = F \in \mathbb{C}^{2^n}$, $|\sigma|+\log(|F|) \leqslant n - c$ and

$$\sum_{v \in F} \langle v|\rho_n|v\rangle > \epsilon.$$

Let $t = n + s$ be the least element of C greater than n. On input σ, M outputs T as above. Note that

$$Q := \sum_{w \in T} |w\rangle\langle w| = \sum_{v \in F, \pi \in 2^s} |v\rangle\langle v| \otimes |\pi\rangle\langle \pi| = \big(\sum_{v \in F} |v\rangle\langle v|\big) \otimes \big(\sum_{\pi \in 2^s} |\pi\rangle\langle \pi|\big) = W \otimes I,$$

where $W := \sum_{v \in F} |v\rangle\langle v|$ and I be the identity on $\mathbb{C}^{2^s}$. Then, by the coherence property of states,

$$\sum_{w \in T} \langle w|\rho_t|w\rangle = \mathrm{Tr}(\rho_t Q) = \mathrm{Tr}(\rho_t[W \otimes I]) = \mathrm{Tr}(\rho_n W) > \epsilon.$$

Consequently,

$$QK^\epsilon(\rho_t) \leqslant |\sigma| + \log(|T|) + l = |\sigma| + \log(|F|) + s + l \leqslant n - c + s + l = t - c + l.$$

Since d and l were constants and c was arbitrary, this contradicts the assumption. □

3.3.3 A weak Levin–Schnorr type result

Theorem 3.11 implies that if ρ is weak-Solovay random then, $\forall \epsilon > 0 \exists c \forall n, QK^\epsilon(\rho_n) > n - c$. I.e., being strong-Solovay random implies the Levin–Schnorr condition. Does this reverse? We give two partial results in this direction: the Levin–Schnorr condition implies that ρ passes all strong-Solovay tests of a certain type.

Definition 3.15. For a rational $s \in (0, 1)$, a s-strong Solovay test is a strong Solovay test $(S^r)_r$ such that $\sum_r \tau(S^r)^s < \infty$ and $\sum_r \tau(S^r)$ is a computable real number.

Theorem 3.16. If $\forall \epsilon > 0 \exists c \forall n, QK^\epsilon(\rho_n) > n - c$, then ρ passes all s-strong Solovay tests for all rational $s \in (0, 1)$.

Proof. Suppose for a contradiction that $(S^m)_m$ is a s-strong Solovay test which ρ fails at $\epsilon > 0$ and $\sum_i \tau(S^i) = Q$, computable. For all m, let S^m be 2^{n_m} by 2^{n_m} and we may let

the n_ms be distinct. Let $f(m) := -\log(\tau(S^m))$ and $g(m) := \lceil sf(m) \rceil$. Partition ω into the fibers induced by g. (P is a fiber of g if $P = g^{-1}(\{x\}) = \{y : g(y) = x\}$, for some x.). Note that $g(r) \geqslant -s\log\tau(S^r)$, and hence $2^{-g(r)} \leqslant \tau(S^r)^s$. In particular, this implies that P is finite. So, there are countably infinitely many fibers, $\{P_1, P_2 \dots\}$ and $\omega = \bigcup_m P_m$, where for all m, there is an x_m such that $P_m = g^{-1}(\{x_m\})$ and $m \mapsto x_m$ is injective.

The fiber P of $x = g(z)$ can be computed from x as follows. Note that $g(c) = x$ iff, $f(c) \in [s^{-1}(x-1), s^{-1}x]$. As Q is computable, compute an interval J such that, $|J| < 2^{-s^{-1}x}$, $Q \in J$ and $\sum_{r \leqslant q} 2^{-f(r)} \in J$ for some q. So, $f(c) > s^{-1}x$ if $c > q$. P can be computed by evaluating g on $[0, q]$.

The idea is to describe S^r by computing the fiber P containing r and then specifying the location of r in the lexicographical ordering on P. As $(S^r)_r$ is a s-strong Solovay test, this description of S^r is short enough to derive a contradiction. Consider the machine, M doing the following: On input λ, check if there is a decomposition $\lambda = \pi\sigma$ such that,

- There is an m such that $\mathbb{U}(\pi) = 0^{g(m)}$.
- $|\sigma| = t = \lceil \log(|P|) \rceil$ where P is the fiber of $g(m)$. (Recall that P can be computed from $g(m)$.)

If these hold, then order P lexicographically using the ordering on 2^t and let r be the σ^{th} element in this ordering. Output F^r where F^r is such that $S^r = \sum_{v \in F^r} |v\rangle\langle v|$.

Note that M is prefix free: Suppose $\lambda, \lambda' \in \mathrm{dom}(M)$ as witnessed by $\lambda = \pi\sigma$ and $\lambda = \pi'\sigma'$. So, M finds m and m' such that $\mathbb{U}(\pi) = 0^{g(m)}$ and $\mathbb{U}(\pi') = 0^{g(m')}$. Let $\pi\sigma \preceq \pi'\sigma'$. Then, it must be that $\pi \preceq \pi'$ or $\pi' \preceq \pi$. Since $\mathbb{U}$ is prefix free, it follows that $\pi = \pi'$. So, $g(m) = g(m')$. Hence, m and m' are in the same fiber, P. Letting $t = \lceil \log(|P|) \rceil$, $\lambda, \lambda' \in \mathrm{dom}(M)$ implies that $|\sigma| = |\sigma'| = t$.

For each $m \in \omega$, let r_m be any element from P_m. Then,

$$\sum_m |P_m| 2^{-g(r_m)} = \sum_m \sum_{r \in P_m} 2^{-g(r)} \leqslant \sum_m \sum_{r \in P_m} \tau(S^r)^s = \sum_i \tau(S^i)^s < \infty. \tag{3.2}$$

Let h be the function defined by, $h(m) := \log(|P_m|) - g(r_m)$ where r_m is any representative from P_m. By (3.2), $|P_m| 2^{-g(r_m)} \to 0$ as $m \to \infty$. So, $h(m) \to -\infty$ as $m \to \infty$. Each fiber is finite and ρ fails the test at ϵ. So, there is an infinite set $I = \{P_{j_1}, P_{j_2}, \dots\}$ such that for all i, there is a $t_i \in P_{j_i}$ with $\mathrm{Tr}(\rho_{n_{t_i}} S^{t_i}) > \epsilon$. $j_i \to \infty$ as $i \to \infty$ and so, $h(j_i) = \log(|P_{j_i}|) - g(r_{t_i}) \to -\infty$ as $i \to \infty$. This asymptotic behavior will be used below to derive a contradiction.

Fix an arbitrary i and a $t = t_i \in P_{j_i}$ as above. So, $\epsilon < \sum_{v \in F^t} \langle v | \rho_{n_t} | v \rangle$.

Let t be the σ^{th} element of P_{j_i} in the lexicographic ordering used by M and let $\mathbb{U}(\pi) = 0^{g(t)}$ and $K(0^{g(t)}) = |\pi|$. Then, $M(\pi\sigma) = F^t$ and so, there is a bitstring ι such that $|\iota| \leqslant^+ K(0^{g(t)}) + \lceil \log(|P_{j_i}|) \rceil$ and $\mathbb{U}(\iota) = F^t$. Note that $\log|F^t| = \log(\mathrm{Tr}(S^t)) = \log(\tau(S^t)) + n_t = -f(t) + n_t$. Let $d := (1-s)s^{-1} > 0$. So, $\{(\lceil nd \rceil, 0^n) : n \in \omega\}$, is a bounded request set (see [21] for a definition) and hence $K(0^n) \leqslant^+ \lceil nd \rceil$. Using all this, we get that:

$$\begin{aligned}
\mathrm{QK}^\epsilon(\rho_{n_t}) &\leqslant^+ K(0^{g(t)}) + \lceil \log(|P_{j_i}|) \rceil - f(t) + n_t \\
&\leqslant^+ \lceil dg(t) \rceil + \lceil \log(|P_{j_i}|) \rceil - f(t) + n_t \\
&\leqslant^+ dsf(t) + \lceil \log(|P_{j_i}|) \rceil - f(t) + n_t \\
&= f(t)(ds - 1) + \lceil \log(|P_{j_i}|) \rceil + n_t \\
&= -sf(t) + \lceil \log(|P_{j_i}|) \rceil + n_t \\
&\leqslant^+ -g(t) + \lceil \log(|P_{j_i}|) \rceil + n_t \\
&= h(j_i) + n_t.
\end{aligned}$$

The last equality follows as $t = t_i$ is in P_{j_i}. This means that there is an infinite sequence $(n_{t_i})_i$ such that

$$\mathrm{QK}^{\epsilon}(\rho_{n_{t_i}}) <^{+} n_{t_i} + h(j_i).$$

Finally, recall that $h(j_i) \to -\infty$ as $i \to \infty$ and we have a contradiction. □

Theorem 3.16 can be strengthened by weakening the defining criteria for a s-strong Solovay test.

Definition 3.17. Let $s \in (0,1)$ be a rational. Let ϕ be any computable, non-decreasing, non-negative function on the reals such that $\phi(sr) \geqslant^{\times} s\phi(r)$ (I.e., there is a $C > 0$ *independent of* s, such that for all r, $C\phi(sr) \geqslant s\phi(r)$) and $\sum_n 2^{-n}\phi(n) < \infty$ (So, ϕ does not tend to infinity too fast). A (ϕ, s)-strong Solovay test is a strong Solovay test $(S^r)_r$ such that

$$\sum_r \frac{\tau(S^r)^s}{\phi(-\log(\tau(S^r)))} < \infty, \tag{3.3}$$

and

$$\sum_r \tau(S^r) = Q,$$

where Q is a computable real number.

The term in the denominator in (3.3) tends to infinity with r and hence it is easier for a strong Solovay test to be a (ϕ, s)-strong Solovay test than to be a s-strong Solovay test. So, passing all (ϕ, s)-strong Solovay tests is a more restrictive notion of randomness than passing all s-strong Solovay tests. So, the following theorem is an improvement of, and implies Theorem 3.16.

Theorem 3.18. If $\forall \epsilon > 0 \exists c \forall n, QK^{\epsilon}(\rho_n) > n - c$, then ρ passes all (ϕ, s)-strong Solovay tests for all rational $s \in (0,1)$ and all ϕ as in Definition 3.17.

Proof. Suppose for a contradiction that $(S^m)_m$ is a (ϕ, s)-strong Solovay test which ρ fails at $\epsilon > 0$ and $\sum_i \tau(S^i) = Q$, computable. For all m, let S^m be 2^{n_m} by 2^{n_m} and we may let the n_ms be distinct. For ease of presentation, we do the proof in 2 cases. First, let $s \leqslant 0.5$. Let $f(m) := -\log(\tau(S^m))$ and let $g(m) := \lceil sf(m) \rceil$. Partition ω into the fibers induced by g. Fix some fiber P of some $x = g(r)$. I.e., r is a representative from P. Then, $g(r) = \lceil s(-\log\tau(S^r)) \rceil$. So, $g(r) \geqslant -s\log\tau(S^r)$, and hence $2^{-g(r)} \leqslant \tau(S^r)^s$. In particular, this implies that each fiber is finite. So, there are countably infinitely many fibers, $\{P_1, P_2 \dots\}$. So, $\omega = \bigcup_m P_m$, where for all m, there is an x_m such that $P_m = g^{-1}(\{x_m\})$ and $m \mapsto x_m$ is injective. For each $m \in \omega$, let r_m be any representative from P_m. For all r, $sf(r) \leqslant g(r)$ and ϕ is non-decreasing. So,

$$\sum_m |P_m| \frac{2^{-g(r_m)}}{\phi(g(r_m))} = \sum_m \sum_{r \in P_m} \frac{2^{-g(r)}}{\phi(g(r))} \leqslant \sum_m \sum_{r \in P_m} \frac{\tau(S^r)^s}{\phi(sf(r))} \leqslant^{\times} \sum_r \frac{\tau(S^r)^s}{s\phi(f(r))} < \infty. \quad (3.4)$$

The fiber P of $x = g(z)$ can be computed from x for the same reason as in the previous proof. Its idea of 'compressing' S^r is also used here.

Consider the machine, M doing the following: On input λ, search for a decomposition $\lambda = \pi\sigma$, such that

- $\mathbb{U}(\pi) = 0^{g(m)}$ for some m.
- $|\sigma| = t$ where P is the fiber containing m, (which can be computed from $g(m)$) and $t = \lceil \log(|P|) \rceil$.

If found, order P lexicographically using the ordering on 2^t and let r be the σ^{th} element in this ordering. Output F^r where F^r is such that $S^r = \sum_{v \in F^r} |v\rangle\langle v|$. Note that M is prefix free for the same reason as in the previous proof. Let l be M's coding constant. Let h be the function defined by, $h(m) := \log(|P_m|) - g(r_m) - \log \phi g(r_m)$, where r_m is

any representative from P_m. By (3.4),

$$\frac{|P_m|2^{-g(r_m)}}{\phi g(r_m)} \to 0$$

as $m \to \infty$. So, $h(m) \to -\infty$ as $m \to \infty$. Each fiber is finite and ρ fails the test at ϵ. So, there is an infinite set $I = \{P_{j_1}, P_{j_2}, \dots\}$ such that for all i, there is a $t_i \in P_{j_i}$ with $\mathrm{Tr}(\rho_{n_{t_i}} S^{t_i}) > \epsilon$. $j_i \to \infty$ as $i \to \infty$ and so, $h(j_i) \to -\infty$ as $i \to \infty$. This asymptotic behavior will be used below to derive a contradiction.

Fix an arbitrary i and a $t = t_i \in P_{j_i}$ as above. So,

$$\epsilon < \sum_{v \in F^t} \langle v|\rho_{n_t}|v\rangle. \tag{3.5}$$

Let t be the σ^{th} element of P_{j_i} in the lexicographic ordering used by M. Let π be such that $K(0^{g(t)}) = |\pi|$ and $\mathbb{U}(\pi) = 0^{g(t)}$. Then, $M(\pi\sigma) = F^t$ and so, there is a bitstring κ such that $|\kappa| \leqslant K(0^{g(t)}) + \lceil \log(|P_{j_i}|) \rceil + l$ and $\mathbb{U}(\kappa) = F^t$. Note that $\log|F^t| = \log(\mathrm{Tr}(S^t)) = \log(\tau(S^t)) + n_t = -f(t) + n_t$. So,

$$\mathrm{QK}^\epsilon(\rho_{n_t}) \leqslant K(0^{g(t)}) + \lceil \log(|P_{j_i}|) \rceil + l - f(t) + n_t.$$

Note that $\{(n - \lceil \log(\phi(n)) \rceil, 0^n) : n \in \omega\}$ is a bounded request set by definition of a (ϕ, s) test and so $K(0^{g(t)}) \leqslant^+ g(t) - \log(\phi g(t))$. So,

$$\mathrm{QK}^\epsilon(\rho_{n_t}) \leqslant^+ g(t) - \log(\phi g(t)) + \lceil \log(|P_{j_i}|) \rceil - f(t) + n_t.$$

Since $g(t) - 1 < sf(t)$, we have

$$-g(t) + 1 > -sf(t). \tag{3.6}$$

Since $s \leqslant 0.5$ we have that $1 - s \geqslant s$.

So, $g(t) - f(t) \leqslant sf(t) - f(t) + 1 = -(1-s)f(t) + 1 \leqslant -sf(t) + 1$. Using (3.6),

$$g(t) - f(t) < -g(t) + 2.$$

So,

$$\mathrm{QK}^{\epsilon}(\rho_{n_t}) <^{+} -g(t) + \lceil \log(|P_{j_i}|) \rceil - \log(\phi g(t)) + n_t = h(j_i) + n_t.$$

The equality follows as $t = t_i$ is in P_{j_i}. This means that there is an infinite sequence $(n_{t_i})_i$ such that $\mathrm{QK}^{\epsilon}(\rho_{n_{t_i}}) <^{+} n_{t_i} + h(j_i)$. Finally, recall that $h(j_i) \to -\infty$ as $i \to \infty$ and we have a contradiction.

Now let $s > 0.5$ and let f, g be as in the previous case. Let $b(m) := \lceil (1-s)f(m) \rceil$ and let $C := \lceil s/(1-s) \rceil + 1$.

Consider the machine M doing the following: on input $\pi 1^y 0 \sigma$, check if the following conditions hold.

- There is m such that $\mathbb{U}(\pi) = 0^{b(m)}$.
- If $x = b(m)$, $J = (s(1-s)^{-1}(x-1), s(1-s)^{-1}x + 1] \cap \omega$ and w is the y^{th} element of J, then there is a z such that $g(z) = w$.
- If P is the fiber of g containing z (P is computable from $w = g(z)$ just as in the previous case) and $t = \lceil \log(|P|) \rceil$, then $|\sigma| = t$

If all the above are met, then order P lexicographically using the ordering on 2^t and let r be the σ^{th} element in this ordering. Output F^r.

Roughly, the idea is as follows: Just as in the previous case, we want to compress F^r where r is the σ^{th} number in the fiber of $w = g(m)$. The first step to achieve this is to describe $g(m)$. While in the previous case we used an ι such that $\mathbb{U}(\iota) = 0^{g(m)}$ and $|\iota| = K(0^{g(m)}))$, we use here the shorter string π where $\mathbb{U}(\pi) = 0^{b(m)}$ and $|\pi| = K(0^{b(m)})$ together with 1^y for describing $g(m)$. From π, we get $x = b(m)$ which in turn gives J which contains $g(m)$. So, π along with y, the location of $g(m)$ in J, describes $g(m)$.

After $g(m)$ is found, F^r can be described just as in the previous case. The details are: As $x = b(m)$, $(1-s)f(m) \in (x-1, x]$ and hence $sf(m)$ lies in $(s(1-s)^{-1}(x-1), s(1-s)^{-1}x]$. So, $\lceil sf(m) \rceil = g(m) \in J = (s(1-s)^{-1}(x-1), s(1-s)^{-1}x+1] \cap \omega$. Since $|J| \leqslant C$, $g(m) \in J$ can be determined by specifying $y \leqslant C$, it's location in J. So, M can recover $g(m)$. From this point on, the remaining procedure is the same as in the previous case.

We see that M is prefix-free: Let $\pi 1^y 0 \sigma$ and $\pi' 1^{y'} 0 \sigma'$ be in the domain of M and let $\pi 1^y 0 \sigma \preceq \pi' 1^{y'} 0 \sigma'$. By the same argument as in case1, $\pi = \pi'$ and M finds some m, m' with $x = b(m) = b(m')$. It follows that $y = y'$. So, if w is the y^{th} (and y'^{th}) element of J (as above), then M finds z, z' such that $g(z) = w = g(z')$. So, z and z' are in the same fiber P and it hence follows as in the previous case that $|\sigma| = |\sigma'|$. Define I and h exactly as in the previous case. Fix some i and let $t = t_i$ be an element of P_{j_i} such that (3.5) holds. Let t be the σ^{th} element of P_{j_i}. Let $x = b(t) = \lceil (1-s)f(t) \rceil$. So, $(1-s)f(t) \in (x-1, x]$ and $sf(t) \in (s(1-s)^{-1}(x-1), s(1-s)^{-1}x]$. Hence, $g(t) \in (s(1-s)^{-1}(x-1), s(1-s)^{-1}x+1] \cap \omega = J$ and let $g(t)$ be the y^{th} element of J. Let π be such that $\mathbb{U}(\pi) = 0^{b(t)}$ and $|\pi| = K(0^{b(t)})$. Then, on input $\pi 1^y 0 \sigma$, M finds some z (it could be that $z = t$, but not necessarily) such that $b(t) = b(z) = x$ and then finds that the y^{th} element of J is $g(z')$ for some z' (again, although $g(z') = g(t)$, it could be that $t = z'$ but not necessarily). Since z' and t are both in P_{j_i}, M outputs F^t after reading σ. So, there is a π such that $\mathbb{U}(\pi) = F^t$ and $|\pi| \leqslant^+ K(0^{b(t)}) + C + \lceil \log(|P_{j_i}|) \rceil$.

So, $\mathrm{QK}^\epsilon(\rho_{n_t})$

$$
\begin{aligned}
&<^+ K(0^{b(t)}) + \lceil \log(|P_{j_i}|) \rceil + \log(|F^t|) \\
&\leqslant^+ b(t) - \lceil \log(\phi(g(t))) \rceil + \lceil \log(|P_{j_i}|) \rceil + n_t - f(t) \\
&\leqslant^+ -g(t) - \lceil \log(\phi(g(t))) \rceil + \lceil \log(|P_{j_i}|) \rceil + n_t
\end{aligned}
$$

The last inequality is since, by (3.6) (which holds for any s), $b(t)-f(t) \leqslant (1-s)f(t)-f(t)+1 = -sf(t)+1 < -g(t)+2$. Since $t = t_i \in P_{j_i}$, we see that $\mathrm{QK}^\epsilon(\rho_{n_t}) <^+ h(j_i)-n_{t_i}$. for all i. This gives a contradiction for the same reason as in the previous case.

□

3.3.4 QK and computable measure machines

Schnorr randomness is an important randomness notion in the classical realm [21, 28]. While K plays well with Solovay randomness, K_C, a version of K using a computable measure machine, C (a prefix-free Turing machine whose domain has computable Lebesgue measure) gives a Levin–Schnorr characterization of Schnorr randomness (See theorem 7.1.15 in [21]).

So, with the intention of connecting it to quantum Schnorr randomness, we define QK_C a version of QK using a computable measure machine, C.

Theorem 3.20 shows that QK_C agrees with K_C on the classical bitstrings. Analogously to the classical case, Theorem 3.22 is a Levin–Schnorr type of characterizations of quantum Schnorr randomness using QK_C. Theorem 3.23, a Chaitin type characterization of quantum Schnorr randomness using QK_C implies Theorem 3.24, a Chaitin type characterization of *classical* Schnorr randomness in terms of K_C.

For C a computable measure machine and σ a string, K_C is defined analogously to K; $K_C(\sigma) :=\inf\{|\tau| : C(\tau) = \sigma\}$. The quantum version is: for C, a computable measure machine and a $\epsilon > 0$, define $QK_C^\epsilon(\tau)$ to be:

Definition 3.19. $QK_C^\epsilon(\tau) := \inf \{|\sigma|+\log|F| : C(\sigma) \downarrow= F$, a orthonormal set in $\mathbb{C}_{alg}^{2^{|\tau|}}$ and $\sum_{v\in F} \langle v|\tau|v\rangle > \epsilon\}$

The infimum of the empty set is taken to be ∞. Notation: In this section, μ denotes Lebesgue measure and C_t denotes C run upto the t steps. We may assume that $\mathrm{dom}(C_t) \subseteq 2^t$. By a *sequence*, we mean a countable collection whose elements may possibly be repeated. If S is a sequence, the sum $\sum_{s\in S}$ will be over all elements of S, with repetition.

Similarly to Theorem 3.2, we show that QK_C 'agrees with' K_C on the classical qubitstrings. In Theorem 3.20 and its proof, P and C will stand for computable measure machines.

Theorem 3.20. For all rational $\epsilon > 0$ and all C, there exists a P such that $K_P(\sigma) \leqslant QK^{\epsilon}_C(|\sigma\rangle\langle\sigma|) + 1$ for all classical bitstrings σ.

Proof. The proof is almost identical to that of Theorem 3.2. Fix a rational $\epsilon > 0$ and a C. Consider the machine P from the proof of Theorem 3.2 but with $\mathbb{U}$ replaced by C. We now show that $\mu(\mathrm{dom}(P))$ is computable. Let $\delta > 0$ be arbitrary. Since $\mu(\mathrm{dom}(C))$ is computable, find a stage t so that $\mu(\mathrm{dom}(C)) - \mu(\mathrm{dom}(C_t)) < \delta$. (The t can be found as follows: Compute a q' such that $|q - q'| < \delta/2$. So, $q' - \delta/2 < q < q' + \delta/2$. Since $\mu(\mathrm{dom}(C_t)) \nearrow q$, as $t \to \infty$, we can compute a t such that, $q' - \delta/2 < \mu(\mathrm{dom}(C_t)) < q' + \delta/2$.). We may compute S, the set of those strings $\pi = \sigma\tau \in \mathrm{dom}(P)$ and $\sigma \in \mathrm{dom}(C_t)$. So, $\mathrm{dom}(P)\backslash S$ consists of strings $\pi = \sigma\tau$ such that $\sigma \in \mathrm{dom}(C)\backslash\mathrm{dom}(C_t)$. So, it is easy to see that $\mu(\mathrm{dom}(P))$-$\mu(S) < \mu(\mathrm{dom}(C))$-$\mu(\mathrm{dom}(C_t)) < \delta$. As $\delta > 0$ was arbitrary, this shows that $\mu(\mathrm{dom}(P))$ is computable. Now, let $\sigma \in 2^n$ be any classical bitstring such that $QK^{\epsilon}_C(|\sigma\rangle\langle\sigma|) < \infty$. Let λ and $F \subseteq \mathbb{C}^{2^n}_{alg}$ orthonormal such that $|\lambda| + \log(|F|) = QK^{\epsilon}_C(|\sigma\rangle\langle\sigma|)$, $\sum_{v\in F} \langle v|\sigma\rangle\langle\sigma|v\rangle > \epsilon$ and $C(\lambda) = F$. Let $O := \sum_{v\in F} |v\rangle\langle v|$. Note that since $\epsilon < \sum_{v\in F} \langle v|\sigma\rangle\langle\sigma|v\rangle = \langle\sigma|O|\sigma\rangle$, $\sigma \in S^{\epsilon}_{E,O}$ where E is

the standard basis. Let τ be a length $\lceil \log(\epsilon^{-1}|F|) \rceil$ string such that $g(\tau) = \sigma$. Then, we see that $P(\lambda\tau) = \sigma$. So,

$$K_P(\sigma) \leqslant |\lambda| + |\tau| \leqslant |\lambda| + \log(\epsilon^{-1}) + 1 + \log(|F|) = QK_C^{\epsilon}(|\sigma\rangle\langle\sigma|) + 1.$$

□

Remark 3.21. Theorem 3.20 establishes one direction of the coincidence of K_C and QK_C for classical qubitstrings. In the other direction, take some classical bitstring σ with $K_C(\sigma) < \infty$ for some C. Let $C(\pi) = \sigma$ and $|\pi| = \mathrm{K}_C(\sigma)$. Then, letting $F = \{\sigma\}$ in 3.19, $QK_C^{\epsilon}(|\sigma\rangle\langle\sigma|) \leqslant QK_C^{1}(|\sigma\rangle\langle\sigma|) \leqslant |\pi| = K_C(\sigma)$, for any $\epsilon > 0$.

3.3.5 Quantum Schnorr randomness and QK_C

Theorem 3.22 is a quantum analogue of the classical characterization of Schnorr randomness: X is Schnorr random if and only if for any computable measure machine, C, there is a constant d such that for all n, $K_C(X \upharpoonright n) > n - d$.

Theorem 3.22. A state ρ is quantum Schnorr random if and only if for any computable measure machine, C and any $\epsilon > 0$, there is a constant $d > 0$ such that for all n, $QK_C^{\epsilon}(\rho_n) > n - d$.

Proof. ($\Rightarrow$) We prove it by contraposition. I.e., show that ρ is not quantum Schnorr random if there is a C and an $\epsilon > 0$ such that for all d, there is an $n = n_d$ such that $QK_C^{\epsilon}(\rho_n) \leqslant n - d$. Let T_s be the set of all σ such that $C_s(\sigma) \downarrow = F_\sigma$, an orthonormal set such that $|\sigma| + \log |F_\sigma| < n_\sigma$ and $F_\sigma \subseteq \mathbb{C}^{2^{n_\sigma}}$ for some n_σ. Let $T = \bigcup_s T_s$. For all strings σ, let $P_\sigma := \sum_{v \in F_\sigma} |v\rangle\langle v|$. Let Q_s be the sequence of those P_σ for $\sigma \in T_s$, Q the sequence of those P_σ for $\sigma \in T$ and D_s the sequence of those P_σ for $\sigma \in T \backslash T_s$. Next, we

show that $\alpha := \sum_{P \in Q} \tau(P)$ is computable by showing how to approximate it within 2^{-k} for an arbitrary k: Computably find a t (using the same method as in Theorem 3.20) such that $\mu(\mathrm{dom}(C)) - \mu(\mathrm{dom}(C_t)) < 2^{-k}$. We show that $\sum_{P_\sigma \in Q_t} \tau(P_\sigma)$ is within 2^{-k} of α. Note that for all $\sigma \in T$, $2^{|\sigma|}|F_\sigma| < 2^{n_\sigma}$. So, $\tau(P_\sigma) = 2^{-n_\sigma}|F_\sigma| < 2^{-|\sigma|}$.

$$\alpha - \sum_{P_\sigma \in Q_t} \tau(P_\sigma) = \sum_{P_\sigma \in D_t} \tau(P_\sigma) = \sum_{\sigma \in T/T_t} |F_\sigma| 2^{-n_\sigma} \leqslant \sum_{\sigma \in T/T_t} 2^{-|\sigma|}$$

$$\leqslant \sum_{\sigma \in \mathrm{dom}(C)/\mathrm{dom}(C_t)} 2^{-|\sigma|} \leqslant (\mu(\mathrm{dom}(C)) - \mu(\mathrm{dom}(C_t))) < 2^{-k}$$

Note that $\sum_{P_\sigma \in Q_t} \tau(P_\sigma)$ is a rational, uniformly computable in t since $\mathrm{dom}(C_t) \subseteq 2^t$ is uniformly computable in t. This shows that Q is a quantum Schnorr test. By the assumption, we see that is a infinite sequence $d_1 < d_2 < \cdots$ and a list of distinct natural numbers $n_{d_1}, n_{d_2} \cdots$ so that for all i, there is a P_i in Q such that $\mathrm{Tr}(P_i \rho_{n_{d_i}}) > \epsilon$. So, ρ fails Q at ϵ.

($\Leftarrow$) We prove it by contraposition. Suppose that ρ fails a quantum-Schnorr test, $(S^r)_r$ at ϵ. For all j, let s_j be the least t such that

$$\sum_{i=0}^{t} \tau(S^i) > \alpha - 2^{-j}.$$

We show how the sequence $(s_j)_j$ can be computed. First, let $\sum_r \tau(S^r) = \alpha$, be a computable real which is not a dyadic rational. s_j may be computed as follows: Note that as α is not a dyadic rational but $\tau(S^i)$ is a dyadic rational for all i, we have that

$$\sum_{i=0}^{s_j - 1} \tau(S^i) < \alpha - 2^{-j} < \sum_{i=0}^{s_j} \tau(S^i).$$

By Proposition 5.1.1 in [21], the left cut, $L(\alpha - 2^{-j})$ of $\alpha - 2^{-j}$ is computable. So, we may search for rationals $q \in L(\alpha - 2^{-j}), q' \notin L(\alpha - 2^{-j})$ and for a t such that,

$$\sum_{i=0}^{t-1} \tau(S^i) \leqslant q < q' \leqslant \sum_{i=0}^{t} \tau(S^i).$$

This t is the needed s_j. Now, let α be a dyadic rational. Then, $\alpha - 2^j$ has a finite binary representation and s_j can be directly computed. So, in summary, the $(s_j)_j$ is a computable sequence, after (non-uniformly) knowing whether α is a dyadic rational or not. For all $r \geqslant 0$, define special projections

$$G_r := \sum_{i=s_r+1}^{s_{r+1}} S^i.$$

So,

$$\tau(G_r) \leqslant \sum_{i=s_r+1}^{\infty} \tau(S^i) = \alpha - \sum_{i=0}^{s_r} \tau(S^i) < 2^{-r}.$$

Notation: Let each S^i be an operator on $\mathbb{C}^{2^{n_i}}$. Let $n_r = \max\{n_i : s_r + 1 \leqslant i \leqslant s_{r+1}\}$. By tensoring with the identity, we may assume that all S^i, for $s_r + 1 \leqslant i \leqslant s_{r+1}$, are operators on $\mathbb{C}^{2^{n_r}}$. Let $F_r \subseteq \mathbb{C}^{2^{n_r}}$ be an orthonormal set of complex algebraic vectors spanning the range of G_r. Define a computable measure machine, C as follows. On input 0^r10, C outputs F_{2r} and on input 0^r11, C outputs F_{2r+1}. C is clearly prefix-free and the measure of its domain is $\sum_r 2^{-r+2}$, which is computable. Since each G_r is a finite sum of the S^is and as ρ fails $(S^i)_i$ at ϵ, there exist infinitely many r such that $\mathrm{Tr}(\rho_{n_r} G_r) > \epsilon$. Since we may let n_r be strictly increasing in r, there are infinitely many such n_r. Fix such an n_r and let $x = \lfloor r/2 \rfloor$ (I.e., $r = 2x$ or $r = 2x + 1$). Then, $\mathrm{QK}^{\epsilon}_C(\rho_{n_r}) \leqslant x + 2 + n_r + \log\tau(G_r) \leqslant x + 2 + n_r - 2x$. So, $\lfloor r/2 \rfloor - 2 \leqslant n_r - \mathrm{QK}^{\epsilon}_C(\rho_{n_r})$. Letting r go to infinity completes the proof.

□

Theorem 3.23 is a Chaitin-type characterization of quantum-Schnorr randomness using QK^{ϵ}_C. Together with Theorem 3.20 and lemma 3.9 in [11], it implies that Schnorr randoms have a Chaitin type characterization in terms of K_C (Theorem 3.24). To the

best of our knowledge, this is the first, albeit simple, instance where results in quantum algorithmic randomness are used to prove a new result in the classical theory.

Theorem 3.23. ρ is quantum Schnorr random if and only if for all computable measure machines C and all ϵ, $\forall d \forall^\infty n$ $\mathrm{QK}^\epsilon_C(\rho_n) > n + d$.

Proof. ($\Rightarrow$) Suppose toward a contradiction that there is a C, an $\epsilon > 0$ and $c > 0$ such that there are infinitely many n with $\mathrm{QK}^\epsilon_C(\rho_n) \leqslant n + c$. Define a quantum Schnorr test Q as follows. Let T_s be the set of all σ such that $C_s(\sigma) \downarrow = F_\sigma$, an orthonormal set such that $|\sigma| + \log |F_\sigma| < n_\sigma + c$ and $F_\sigma \subseteq \mathbb{C}^{2^{n_\sigma}}$ for some n_σ. Let $T = \bigcup_s T_s$. For all strings σ, let $P_\sigma := \sum_{v \in F_\sigma} |v\rangle\langle v|$. Let Q_s be the sequence of those P_σ for $\sigma \in T_s$ and Q the sequence of those P_σ for $\sigma \in T$. That Q is a quantum Schnorr test is shown by replacing 2^{-k} by 2^{-k-c} in the $\Longrightarrow$ direction of the proof of Theorem 3.22. For any n such that $\mathrm{QK}^\epsilon_C(\rho_n) < n + c$, there is a $\sigma \in T$ such that $\mathrm{Tr}(P_\sigma \rho_n) > \epsilon$. So, ρ fails Q at ϵ.

($\Leftarrow$) If ρ is not quantum Schnorr random then by Theorem 3.22, there is a C and an ϵ such that $\forall d \exists n$ such that $\mathrm{QK}^\epsilon_C(\rho_n) \leqslant n - d$. □

We now show the classical version of Theorem 3.23.

Theorem 3.24. An infinite bitstring X is quantum Schnorr random if and only if for all computable measure machines C, $\forall d \forall^\infty n$ $\mathrm{K}_C(X \upharpoonright n) > n + d$.

Proof. ($\Longrightarrow$) : Suppose first that X is Schnorr random. Then, $\rho := \rho_X$, the state induced by X is quantum Schnorr random by lemma 3.9 in [11]. Suppose for a contradiction that there is a C and a d such that $\exists^\infty n$ such that $K_C(X \upharpoonright n) \leqslant n + d$. By Remark 3.21, $\exists^\infty n$ such that $QK^{0.5}_C(\rho_n) \leqslant n + d$, contradicting Theorem 3.23. ($\Longleftarrow$) : Suppose that X is not Schnorr random. Once again, by lemma 3.9 in [11], we have that $\rho := \rho_X$ is not

quantum Schnorr random. By Theorem 3.23, there is a C, an ϵ and a d such that $\exists^\infty n$ such that $\mathrm{QK}^\epsilon_C(\rho_n) \leqslant n + d$. By Theorem 3.20, there is a P such that $\exists^\infty n$ such that $K_P(\rho_n) \leqslant n + d + 1$, a contradiction. $\square$

Chapter 4

Generating classical randomness from a non-quantum random state

4.1 Introduction

This chapter investigates the following question: Can the quantum non-randomness of a state always be detected using qubitbitwise measurements? We show that it is not always possible to do so by constructing a computable, non-qMLR state ρ which yields a Martin-Löf random bitstring with probability one when measured qubitwise. I.e., the quantum non-randomness of ρ cannot be detected by qubitwise measurements as these yield a random bitstring almost surely.

We first formalize our main question in the language of quantum algorithmic randomness [11,31]. While versions of this question have been studied in the past [1,3–5,25,33], this work is the first one to study it using notions from quantum algorithmic randomness.

We let 2^ω denote Cantor space (the collection of infinite sequences of bits), let 2^n denote the set of bit strings of length n, $2^{<\omega} := \bigcup_n 2^n$ and let $2^{\leqslant\omega} := 2^{<\omega} \cup 2^\omega$. Martin-Löf randomness (MLR) and Quantum-Martin-Löf randomness (q-MLR) has been defined already in previous chapters. Our motivating question can now be framed as: Is there a computable, non q-MLR state which can be used to 'generate' a MLR sequence of bits.

To make the question fully precise, we define 'generate'.

Measuring a finite dimensional quantum system is a pivotal concept in quantum theory [17]. It hence seems natural to extend the notion of measurement from finite dimensional systems to states, which are coherent, increasing sequences of finite dimensional systems. We define (see Section 4.2) such a notion and explain how measuring a state yields an infinite bitstring. With this notion in hand, our main question assumes the precise form: Is there a computable, non q-MLR state which yields a MLR bitstring with probability one when measured?

We give an overview of the chapter. Section 4.2 formalizes how 'measurement' of a state in a computable basis induces a probability measure on Cantor space. Section 4.3 introduces the key notion of measurement randomness for states. A state is defined to be 'measurement random' (mR) if the measure induced by it, under any computable basis, assigns probability one to the set of Martin-Löf randoms. Equivalently, a state is mR if and only if measuring it in any computable basis yields a Martin-Löf random with probability one.

We then show that quantum-Martin-Löf random states are mR. As an answer to our main question, we show in Section 4.4 that the converse fails: there is a computable mR state, ρ which is not quantum-Martin-Löf random. In fact, something stronger is true. Measuring ρ in any computable basis yields an *arithmetically* random sequence with probability one. Our result hence provides a scheme for generating randomness from a quantum source. To the best of our knowledge, none of the schemes proposed so far [1, 3–5, 25, 33] generate arithmetic randomness.

Section 4.6 shows that mR is equivalent to q-MLR for a certain special class of states.

Let $A \in 2^\omega$. We define an A-computable function to be a total function that can

be realized by a Turing machine with A as an oracle. By 'computable', we will refer to $\varnothing$-computable. The concept of an A-computable sequence of natural numbers will come up frequently in our discussion.

Definition 4.1. A sequence $(a_n)_{n\in\mathbb{N}}$ is said to be A-computable if there is a A-computable function ϕ such that $\phi(n) = a_n$

4.2 Measuring a state

To fix notation, let $X(n)$ denote the nth bit of an $X \in 2^{\leqslant\omega}$, let $p(E)$ stand for the probability of the event E.

Definition 4.2. An A-computable measurement system $B = ((b_0^n, b_1^n))_{n=1}^{\infty}$ (or just 'measurement system' for short) is a sequence of orthonormal bases for $\mathbb{C}^2$ such that each b_i^n is complex algebraic and the sequence $((b_0^n, b_1^n))_{n=1}^{\infty}$ is A-computable.

Let $\rho = (\rho_n)_{n=1}^{\infty}$ be a state and $B = ((b_0^n, b_1^n))_{n=1}^{\infty}$ be a measurement system. We now work towards formalizing a notion of *qubitwise* measurement of ρ in the bases in B. A (probability) premeasure [21],p (also called a measure representation [28]), is a function from the set of all finite bit strings to $[0, 1]$ satisfying $\forall n$, $\forall \tau \in 2^n, p(\tau) = p(\tau 0) + p(\tau 1)$. p induces a measure on 2^ω which is seen to be unique by Carathéodory's extension theorem (See 6.12.1 in [21]). Flipping a $0, 1$ sided fair coin repeatedly induces a probability measure (which happens to be the uniform measure) on 2^ω as follows. Let the random variable $Z(n)$ denote the outcome of the the nth coin flip. The sequence $(Z(n))_{n\in\mathbb{N}}$ induces a premeasure, p, on $2^{<\omega}$ which extends to the uniform measure on 2^ω. Here, $p(\sigma) = 2^{-n}$ is the probability that $Z(i) = \sigma(i)$ for all $i \leqslant |\sigma|$. Similarly the act of

measuring ρ qubit by qubit in B induces a premeasure on $2^{<\omega}$ which extends to a probability measure (denoted μ_ρ^B) on 2^ω as follows. Let the random variable $X(n)$ be the $0,1$ valued outcome of the measurement of the nth qubit of ρ. Let p be the premeasure induced by the sequence $(X(n))_{n\in\mathbb{N}}$ on $2^{<\omega}$. p extends to μ_ρ^B on 2^ω. For any $A \subseteq 2^\omega$, $\mu_\rho^B(A)$ is the probability that $X \in A$ where X is the element of 2^ω obtained in the limit by the qubit by qubit measurement of ρ in B. The most conspicuous difference between the two situations is that while the $(Z(n))_{n\in\mathbb{N}}$ are independent, $(X(n))_{n\in\mathbb{N}}$ need not be independent as the elements of ρ can be entangled. We now formalize the above. The following calculations follow from standard results mentioned, for example, in [17].

We now define $(X(n))_{n\in\mathbb{N}}$ and p, the induced premeasure. Measure ρ_1 by the measurement operators $\{|b_0^1\rangle\langle b_0^1|, |b_1^1\rangle\langle b_1^1|\}$ and define $X(1) := i$ where $i \in \{0,1\}$ is such that b_i^1 was obtained by the above measurement. Let $\hat{\rho_2}$ be the density matrix corresponding to the post-measurement state of ρ_2 given that ρ_2 yields $|b^1_{X(1)}\rangle\langle b^1_{X(1)}| \otimes I$ if measured in the system

$$(|b_i^1\rangle\langle b_i^1| \otimes I)_{i\in\{0,1\}}.$$

I.e,

$$\hat{\rho_2} = \frac{(|b^1_{X(1)}\rangle\langle b^1_{X(1)}| \otimes I)\rho_2(|b^1_{X(1)}\rangle\langle b^1_{X(1)}| \otimes I)}{tr((|b^1_{X(1)}\rangle\langle b^1_{X(1)}| \otimes I)\rho_2)}.$$

To define $X(2)$, measure $\hat{\rho_2}$ by the measurement operators

$$(I \otimes |b_i^2\rangle\langle b_i^2|)_{i\in\{0,1\}},$$

and set $X(2) := i$ where $i \in \{0,1\}$ is such that $I \otimes |b_i^2\rangle\langle b_i^2|$ is obtained after the measurement. We use $\hat{\rho_2}$ instead of ρ_2 to define $X(2)$ to account for the previous measurement of the first qubit. $X(n)$ is defined similarly. By the above,

$$p(ij) := p(X(1) = i, X(2) = j) = p(X(1) = i)p(X(2) = j|X(1) = i) =$$

$$p(X(1)=i)tr\big[I\otimes|b_j^2\rangle\langle b_j^2|(\frac{(|b_i^1\rangle\langle b_i^1|\otimes I)\rho_2(|b_i^1\rangle\langle b_i^1|\otimes I)}{tr((|b_i^1\rangle\langle b_i^1|\otimes I)\rho_2)})\big].$$

Since $PT_{\mathbb{C}^2}(\rho_2)=\rho_1$, $p(X(1)=i)=tr\big((|b_i^1\rangle\langle b_i^1|\otimes I)\rho_2\big)$. So,

$$p(ij)=tr\big[\rho_2(|b_i^1b_j^2\rangle\langle b_i^1b_j^2|)\big].$$

Given $\tau\in 2^n$, similar calculations show that

$$p(\tau):=p(X(1)=\tau(1),\ldots,X(n)=\tau(n))=tr\big[\rho_n(|\bigotimes_{i=1}^n b^i_{\tau(i)}\rangle\langle\bigotimes_{i=1}^n b^i_{\tau(i)}|\big]. \tag{4.1}$$

This defines p. The following lemma shows that $p(.)$ is a premeasure. Define μ_ρ^B to be the unique probability measure induced by it.

Lemma 4.3. $\forall n,\ \forall\tau\in 2^n, p(\tau)=p(\tau 0)+p(\tau 1)$

Proof. Noting that for $j\in\{0,1\}$,

$$\rho_{n+1}(|\bigotimes_{i=1}^n b^i_{\tau(i)}\otimes b_j^{n+1}\rangle\langle\bigotimes_{i=1}^n b^i_{\tau(i)}\otimes b_j^{n+1}|)=\rho_{n+1}(|\bigotimes_{i=1}^n b^i_{\tau(i)}\rangle\langle\bigotimes_{i=1}^n b^i_{\tau(i)}|\otimes|b_j^{n+1}\rangle\langle b_j^{n+1}|),$$

and letting $A:=|\bigotimes_{i=1}^n b^i_{\tau(i)}\rangle\langle\bigotimes_{i=1}^n b^i_{\tau(i)}|$, the right hand side is

$$=tr\big[(A\otimes|b_0^{n+1}\rangle\langle b_0^{n+1}|)\rho_{n+1}+(A\otimes|b_1^{n+1}\rangle\langle b_1^{n+1}|)\rho_{n+1}\big]$$

$$=tr\big[(A\otimes(|b_0^{n+1}\rangle\langle b_0^{n+1}|+|b_1^{n+1}\rangle\langle b_1^{n+1}|))\rho_{n+1}\big]=tr\big[(A\otimes I)\rho_{n+1}\big]=tr[A\rho_n]=p(\tau)$$

□

Remark 4.4. If B is S-computable and ρ is T-computable, then the sequence $\{\mu_\rho^B(\sigma)\}_{\sigma\in\mathbb{N}}$ is $S\oplus T$-computable.

Here, $S\oplus T$ is obtained by putting S on the even bits and T on the odd bits [28].

4.3 Measurement randomness

Let $MLR \subset 2^\omega$ be the set of MLR bitstrings. If ρ is a state and B a measurement system, $\mu_\rho^B(MLR)$ is the probability of getting a MLR bitstring by a qubit-wise measurement of ρ as described in the previous section.

Definition 4.5. ρ is measurement random (mR) if for any computable measurement system, B, $\mu_\rho^B(MLR) = 1$

Theorem 4.6. All q-MLR states are also mR states.

Proof. Let $\rho = (\rho_n)_{n\in\mathbb{N}}$ be q-MLR. Suppose towards a contradiction that there is a $\delta \in (0,1)$ and a computable $B = ((b_0^n, b_1^n))_{n=1}^\infty$ such that $\mu_\rho^B(2^\omega/MLR) > \delta$. Let $(S^m)_m$ be the universal MLT [28] and let for all m,

$$S^m = \bigcup_{m\leqslant i} [\![A_i^m]\!], \tag{4.2}$$

where the A_i^ms satisfy the conditions of Definition 1.6. By the definition of a MLT, for all m and all $i \geqslant m$, we can write $A_i^m = \{\tau_1^{m,i}, \ldots, \tau_{k^{m,i}}^{m,i}\} \subset 2^i$ for some $0 \leqslant k^{m,i} \leqslant 2^{i-m}$. Now define a q-MLT as follows. For all m and $i \geqslant m$, let $\tau_a = \tau_a^{m,i}$ for convenience and define the special projection:

$$p_i^m = \sum_{a\leqslant k^{m,i}} (|\bigotimes_{q=1}^{i} b_{\tau_a(q)}^q\rangle\langle\bigotimes_{q=1}^{i} b_{\tau_a(q)}^q|). \tag{4.3}$$

Letting $P^m := (p_i^m)_{m\leqslant i}$, we see that $(P^m)_{m\in\mathbb{N}}$ is a q-MLT (For each m, the sequence $(p_i^m)_{m\leqslant i}$ is computable since B and $(A_i^m)_{m\leqslant i}$ are computable. Condition 3 in Definition 1.6 implies that for all i, range(p_i^m) $\subseteq$range(p_{i+1}^m). So, P^m is a q-Σ_0^1 class for all m. $k^{m,i} \leqslant 2^{i-m}$ for all m, i implies that $\tau(P^m) \leqslant 2^{-m}$ for all m. Since $(S^m)_{m\in\mathbb{N}}$ is a MLT, $(P^m)_{m\in\mathbb{N}}$ is a computable sequence.) For all m, $(2^\omega/MLR) \subseteq S^m$ holds by the definition

of a universal MLT. Hence, since 4.2 is an increasing union and as $\mu_\rho^B(2^\omega/MLR) > \delta$, for all m there exists an $i(m) > m$ such that

$$\mu_\rho^B([\![A^m_{i(m)}]\!]) > \delta. \tag{4.4}$$

Fix such an m and corresponding $i = i(m)$ and let $A^m_i = \{\tau_1, \ldots, \tau_{k^{m,i}}\}$ for some $k^{m,i} \leqslant 2^{i-m}$ as in 4.3. By 4.1 and 4.4, we have that

$$\delta < \sum_{a \leqslant k} p(\tau_a) = \sum_{a \leqslant k^{m,i}} tr\big[\rho_i(|\bigotimes_{q=1}^{i} b^q_{\tau_a(q)}\rangle\langle\bigotimes_{q=1}^{i} b^q_{\tau_a(q)}|)\big] = tr\big[\rho_i \sum_{a \leqslant k^{m,i}} (|\bigotimes_{q=1}^{i} b^q_{\tau_a(q)}\rangle\langle\bigotimes_{q=1}^{i} b^q_{\tau_a(q)}|)\big] \tag{4.5}$$

So, by 4.3 and 4.5, we see that for all m there is an i such that,

$$\delta < tr[\rho_i p^m_i] \leqslant \rho(P^m).$$

So, $\inf_m(\rho(P^m)) > \delta$, contradicting that ρ is q-MLR. □

Definition 4.7. $\rho = (\rho_n)_{n\in\mathbb{N}}$ is computable if the sequence $(\rho_n)_{n\in\mathbb{N}}$ is computable.

4.4 A measurement random, non q-MLR state

We show that Theorem 4.6 does not reverse:

Theorem 4.8. There is a computable state which is not q-MLR but is mR.

Proof. All matrices in this proof are in the standard basis. Let $\rho = \bigotimes_{n=5}^{\infty} d_n$ and for $N > 5$, $S_N := \bigotimes_{n=5}^{N} d_n$. where d_n is a 2^n by 2^n matrix with 2^{-n} along the diagonal and $r_n := \lfloor 2^n/n \rfloor$ many 2^{-n}s on the extreme ends of the anti-diagonal. Formally, define d_n to be the symmetric matrix such that: For $i \leqslant r_n$, $d_n(i,j) = 2^{-n}$ if $j = i$ or $j = 2^n - i + 1$

and $d_n(i,j) = 0$ otherwise. For $r_n < i < 2^n - r_n$, $d_n(i,j) = 2^{-n}$ if $j = i$ and $d_n(i,j) = 0$ otherwise. For example, $r_3 = 2$ and so,

$$d_3 = \begin{bmatrix} 2^{-3} & 0 & 0 & 0 & 0 & 0 & 0 & 2^{-3} \\ 0 & 2^{-3} & 0 & 0 & 0 & 0 & 2^{-3} & 0 \\ 0 & 0 & 2^{-3} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2^{-3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2^{-3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2^{-3} & 0 & 0 \\ 0 & 2^{-3} & 0 & 0 & 0 & 0 & 2^{-3} & 0 \\ 2^{-3} & 0 & 0 & 0 & 0 & 0 & 0 & 2^{-3} \end{bmatrix}$$

Clearly, d_n is a density matrix. The theorem will be proved via the following lemmas.

Lemma 4.9. ρ is not q-MLR.

Proof. It is easy to see that zero has multiplicity r_n as an eigenvalue of d_n. Hence, letting $q_n = 2^n - r_n$, the eigenpairs of d_n can be listed as $\{\alpha_i^n, v_i^n\}_{i=1}^{2^n}$ where $\alpha_i^n = 0$ if $q_n + 1 \leqslant i \leqslant 2^n$ and $(v_i^n)_{i=1}^{2^n}$ is a orthonormal basis of $\mathbb{C}^{2^n}$.

Fix a $N > 5$. By properties of the Kronecker product, S_N has a orthonormal basis of eigenvectors:

$$\{\bigotimes_{n=5}^{N} v_{l(n)}^n : (l(n))_{n=5}^N \text{ is a sequence such that for all } n, l(n) \leqslant 2^n\},$$

and $\bigotimes_{n=5}^N v_{l(n)}^n$ has eigenvalue $\prod_{n=5}^N \alpha_{l(n)}^n$. Letting M_N be those elements of the above eigenbasis having non-zero eigenvalues, we have that

$$M_N = \{\bigotimes_{n=5}^{N} v_{l(n)}^n : (l(n))_{n=5}^N \text{ is a sequence such that for all } n, l(n) \leqslant q_n\}. \tag{4.6}$$

(See Remark 4.13 for an intuitive explanation of the reason for choosing such an M_N.) By the definition of q_n,

$$|M_N| = \prod_{n=5}^{N} 2^n - \lfloor 2^n/n \rfloor \leqslant \prod_{n=5}^{N} 2^n - (2^n/n) + 1 = \prod_{n=5}^{N} 2^n(1 - n^{-1} + 2^{-n}) = \prod_{n=5}^{N} 2^n \prod_{n=5}^{N} (1 - n^{-1} + 2^{-n}).$$

Noting that $\prod_{n=5}^{\infty}(1 - n^{-1} + 2^{-n}) = 0$, define a q-MLT $(T_m)_{m\in\mathbb{N}}$ as follows. Given m, we describe the construction of T_m. Find $N = N(m)$ such that $\prod_{n=5}^{N}(1 - n^{-1} + 2^{-n}) < 2^{-m}$. Let $\gamma(N) := \sum_{n=5}^{N} n$ and let

$$p_{\gamma(N)} = \sum_{v\in M_N} |v\rangle\langle v|.$$

$p_{\gamma(N)}$ is a special projection on $\mathbb{C}^{2^{\gamma(N)}}$ having rank equal to $|M_N|$. Let $p_k = \varnothing$ for $k < \gamma(N)$ and

$$p_k := p_{\gamma(N)} \otimes \bigotimes_{i=1}^{k-\gamma(N)} I$$

for $k > \gamma(N)$. Using that ρ is computable, it is easy to see that $(p_k)_{k\in\mathbb{N}}$ is a q-Σ_1^0 class. Let $T_m := (p_k)_{k\in\mathbb{N}}$. $(T_m)_{m\in\mathbb{N}}$ is a q-MLT since the choice of $N(m)$ implies that $\tau(T_m) < 2^{-m}$ and as $N(m)$ can be computed from m. $(T_m)_{m\in\mathbb{N}}$ demonstrates that ρ is not q-MLR as follows. Fix m arbitrarily and let $N(m)$ be as above. Recalling that M_N is the set consisting of all eigenvectors of S_N with non-zero eigenvalue, we have that,

$$\rho(T_m) \geqslant tr(\rho_{\gamma(N)} p_{\gamma(N)}) = tr(S_N p_{\gamma(N)}) = tr(S_N) = 1.$$

Since m was arbitrary, $inf_{m\in\mathbb{N}}(\rho(T_m)) = 1$. □

The following technical lemma, although seems unmotivated at this juncture, is crucial at a later point in the proof.

Lemma 4.10. Let $\{[a_i, b_i]^T\}_{i=1}^{n}$ be a set of unit column vectors in $\mathbb{C}^2$. Let $V = \bigotimes_{i=1}^{n}[a_i, b_i]^T$ be their Kronecker product. If $V = [v_1, v_2, \ldots, v_{2^n}]^T$, then for all $k \leqslant 2^{n-1}$,

we have that

$$|v_k||v_{2^n-k+1}| = \prod_{i=1}^{n} |a_i||b_i|.$$

Proof. For natural numbers u and q, let $[u]_q$ denote the remainder obtained by dividing u by q. We use the following convention for the Kronecker product [34]:

$$\begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \otimes \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 \\ b_1 a_2 \\ a_1 b_2 \\ b_1 b_2 \end{bmatrix}.$$

So, $v_1 = \prod_{i=1}^{n} a_i$ and $v_{2^n} = \prod_{i=1}^{n} b_i$. For any $k \leqslant 2^{n-1}$, v_k has the form $v_k = \prod_{i=1}^{n} c_i^k$, for some $c_i^k \in \{a_i, b_i\}$ and v_{2^n-k+1} has the form $v_{2^n-k+1} = \prod_{i=1}^{n} e_i^k$, for some $e_i^k \in \{a_i, b_i\}$. Note that $c_1^k = a_1$ if and only if k is odd if and only if $e_1^k = b_1$. Similarly, we have the following. $c_2^k = a_2$ if and only if $[k]_{2^2} \in \{1, 2\}$ if and only if $e_2^k = b_2$. $c_3^k = a_3$ if and only if $[k]_{2^3} \in \{1, \ldots, 2^2\}$ if and only if $e_3^k = b_3$. In general, for $i \leqslant n$, for all $k \leqslant 2^{n-1}$,

$$c_i^k = a_i \iff [k]_{2^i} \in \{1, \ldots, 2^{i-1}\} \iff e_i^k = b_i.$$

This proves the lemma. Intuitively, this happens for the following reason. Imagine moving from v_1 to $v_{2^{n-1}}$ (by incrementing k) and keeping track of the values of c_i^k as you move along the v_ks. Also, imagine moving from v_{2^n} to $v_{2^{n-1}}$ and keeping track of the values of e_i^k as you move along the v_{2^n-k+1}s. Both motions are in opposite directions since as k is incremented, the first motion is from lower to higher indices and the second is from higher to lower indices. Consider the behavior of c_1^k, e_1^k as k is incremented. At the 'start' point, $c_1^1 = a_1$, $e_1^1 = b_1$. Now, as you move (i.e as you increment k), c_1^k alternates between a_1 and b_1 equalling it's starting value, a_1 at odd ks and e_1^k alternates

between b_1 and a_1 equalling it's starting value b_1 for odd ks. Now, take any $i \leqslant n$. c_i^k alternates between a_i and b_i in blocks of length 2^{i-1}. $c_i^k = a_i$ when k is in the first block, $\{1, 2, \ldots, 2^{i-1}\}$ (i.e, when $[k]_{2^i} \in \{1, 2, \ldots, 2^{i-1}\}$) and $c_i^k = b_i$ when k is in the second block, $\{2^{i-1}+1, \ldots, 2^i\}$(i.e, when $[k]_{2^i} \in \{2^{i-1}+1, \ldots, 0\}$) and so on. Similarly, e_i^k alternates between b_i and a_i in blocks of length 2^{i-1}. □

Lemma 4.11. Let $n \in \mathbb{N}$ and let $\{[a_i, b_i]^T\}_{i=1}^n$ be such that for all i, $[a_i, b_i]^T$ is unit column vector in $\mathbb{C}^2$ and let $W = \bigotimes_{i=1}^n [a_i, b_i]^T$. Then, $|\langle W|d_n|W\rangle| \in [2^{-n}(1-2n^{-1}), 2^{-n}(1+2n^{-1})]$

Proof. Fix n and V as in the statement and write d_n as a block matrix with each block of size 2^{n-1} by 2^{n-1}.

$$d_n = \begin{bmatrix} A & B \\ B^T & A \end{bmatrix}.$$

Letting $V = \bigotimes_{i=1}^{n-1} [a_i, b_i]^T$, in block form, $W = [a_n V^T, b_n V^T]^T$. Let $V = [v_1, v_2, \ldots, v_{2^{n-1}}]^T$. It is easily checked that

$$\langle W|d_n|W\rangle = 2^{-n} + a_n^* b_n V^\dagger B V + a_n b_n^* V^\dagger B^T V.$$

By the form of B we get,

$$V^\dagger B V = 2^{-n}[v_1^*, v_2^*, \ldots, v_{2^{n-1}}^*][v_{2^{n-1}}, v_{2^{n-1}-1}, \ldots, v_{2^{n-1}-r_n+1}, 0, \ldots, 0]^T.$$

$$= 2^{-n} \sum_{k=1}^{r_n} v_k^* v_{2^{n-1}-k+1}.$$

By the previous lemma,

$$|V^\dagger B V| \leqslant 2^{-n} \sum_{k=1}^{r_n} |v_k||v_{2^{n-1}-k+1}| = 2^{-n} r_n \prod_{i=1}^{n-1} |a_i||b_i| = 2^{-n} r_n \prod_{i=1}^{n-1} |a_i|\sqrt{1-|a_i|^2}.$$

Since $x\sqrt{1-x^2}$ has a maximum value of $1/2$ and recalling definition of r_n,

$$|V^\dagger BV| \leqslant 2^{-n}\frac{1}{2^{n-1}}\frac{2^n}{n} = \frac{2^{1-n}}{n}.$$

Similarly, $|V^\dagger B^T V| \leqslant \dfrac{2^{1-n}}{n}$. Noting that $|a_n^* b_n|, |a_n b_n^*| \leqslant 1/2$,

$$|\langle W|d_n|W\rangle| \leqslant 2^{-n} + |a_n^* b_n V^\dagger BV| + |a_n b_n^* V^\dagger B^T V| \leqslant 2^{-n} + \frac{2^{1-n}}{n},$$

and

$$|\langle W|d_n|W\rangle| \geqslant 2^{-n} - |a_n^* b_n V^\dagger BV| - |a_n b_n^* V^\dagger B^T V| \geqslant 2^{-n} - \frac{2^{1-n}}{n}.$$

□

Lemma 4.12. ρ is mR.

If p is any measure on 2^ω, we can define Martin-Löf randomness with respect to p exactly as we defined it for the uniform measure. Denote by $MLR(p)$, the set of bitstrings Martin-Löf random with respect to p [22].

Proof. We use ideas similar to Theorem 196(a) in [22]. For convenience, for all $i > 5$, define

$$\beta_i := \sum_{q=5}^{i-1} q.$$

Let B be any computable measurement system. We show that $MLR(\mu_\rho^B) \subseteq MLR$. Since $\mu_\rho^B[MLR(\mu_\rho^B)] = 1$, this implies that $\mu_\rho^B(MLR) = 1$. Denote μ_ρ^B by μ for convenience. Let λ denote the uniform measure. We will abuse notation by writing $\mu(\tau)$ instead of the more cumbersome $\mu([\![\tau]\!])$ for $\tau \in 2^{<\omega}$. Let $X \in MLR(\mu)$. Write X as a concatenation of finite bitstrings : $X = \sigma_5\sigma_6 \ldots \sigma_n \ldots$ where $\sigma_n \in 2^n$ for all $n \in \mathbb{N}$. Let $S_n := \sigma_5\sigma_6 \ldots \sigma_n$

be the concatenation upto n. Let μ_i be such that for all $\tau \in 2^i$,

$$\mu_i(\tau) := tr\big[d_i(|\bigotimes_{q=1}^{i} b_{\tau(q)}^{q+\beta_i}\rangle\langle\bigotimes_{q=1}^{i} b_{\tau(q)}^{q+\beta_i}|)\big].$$

By 4.1 and by the form of ρ we see that,

$$\mu(S_n) = \prod_{i=5}^{n} \mu_i(\sigma_i).$$

Note that μ is computable [22] since ρ and B are. Since $X \in MLR(\mu)$, by the Levin-Schnorr theorem (Theorem 90, section 5.6 in [22]) there is a C_1 such that

$$\forall n, -\log(\mu(S_n)) - C_1 \leqslant KM(S_n).$$

By Theorem 89, section 5.6 in [22] fix a C_2 such that

$$\forall n, KM(S_n) \leqslant -\log(\lambda(S_n)) + C_2.$$

By these inequalities and taking exponents, we see that there is a constant $\alpha > 0$ such that

$$\forall n, \mu(S_n) \geqslant \alpha\lambda(S_n).$$

Letting $r_i := \mu_i(\sigma_i)$ and $\delta_i := \lambda(\sigma_i) - r_i$ in the above,

$$\forall n, \prod_{i=5}^{n} r_i \geqslant \alpha \prod_{i=5}^{n} r_i + \delta_i. \tag{4.7}$$

Let μ' be a probability measure on 2^ω such that for all $\sigma \in 2^{<\omega}, \mu'(\sigma) := 2\mu(\sigma) - \lambda(\sigma)$. In particular, this implies that

$$\forall n, \mu'(S_n) = \prod_{i=5}^{n} r_i - \delta_i.$$

Note that μ' is computable since μ and λ are. Applying the same argument which resulted in 4.7, we get that there is an $\epsilon > 0$ such that,

$$\forall n, \prod_{i=5}^{n} r_i \geqslant \epsilon \prod_{i=5}^{n} r_i - \delta_i. \tag{4.8}$$

By Lemma 4.11, for all $i, r_i \in [2^{-i}(1-2i^{-1}), 2^{-i}(1+2i^{-1})]$. So, $|\delta_i| = |r_i - 2^{-i}| \in [0, 2^{-i+1}i^{-1}]$. Hence,

$r_i + \delta_i \geqslant 2^{-i} - 2^{-i+1}i^{-1} - 2^{-i+1}i^{-1} = 2^{-i}[1-4i^{-1}] > 0$, since $i \geqslant 5$. Similarly, $r_i - \delta_i \geqslant 0$.

By this, multiplying 4.7 and 4.8 gives,

$$\forall n, \prod_{i=5}^{n} r_i^2 \geqslant \alpha\epsilon \prod_{i=5}^{n} r_i^2 - \delta_i^2 = \alpha\epsilon \prod_{i=5}^{n} r_i^2 \prod_{i=5}^{n} \big(1 - \frac{\delta_i^2}{r_i^2}\big). \tag{4.9}$$

By the above,

$$\frac{|\delta_i|}{r_i} \leqslant \frac{2^{-i+1}i^{-1}}{2^{-i}(1-2i^{-1})} = 2(i-2)^{-1}.$$

Letting $F > 0$ be the constant,

$$\forall n, \prod_{i=5}^{n} \big(1 - \frac{\delta_i^2}{r_i^2}\big) \geqslant \prod_{i=5}^{\infty} \big(1 - \frac{\delta_i^2}{r_i^2}\big) \geqslant \prod_{i=5}^{\infty} \big(1 - 4(i-2)^{-2}\big) = F,$$

4.9 gives,

$$\forall n, (\alpha\epsilon)^{-1} \prod_{i=5}^{n} r_i^2 \geqslant \prod_{i=5}^{n} r_i^2 - \delta_i^2 \geqslant \prod_{i=5}^{n} r_i^2 F. \tag{4.10}$$

From 4.7, 4.8 and 4.10, it is easy to see that there is a $G > 0$ such that for all n

$$\prod_{i=5}^{n} r_i + \delta_i \geqslant G \prod_{i=5}^{n} r_i.$$

Recalling the definitions of r_i and δ_i,

$$\forall n, \lambda(S_n) \geqslant G\mu(S_n).$$

Letting $D = C_1 - \log(G)$ and recalling the definition of C_1,

$$\forall n, -\log(\lambda(S_n)) \leqslant -\log(\mu(S_n)) - \log(G) \leqslant KM(S_n) + D.$$

By Theorem 85 in [22], $KM(.) \leqslant K(.) + O(1)$ and so there is a $E > 0$ such that

$$\forall n, -\log(\lambda(S_n)) \leqslant K(S_n) + E.$$

Noting that $-\log(\lambda(S_n)) = |S_n| = \beta_n + n$, 3.2.14 from [28] implies that X is MLR. $\square$

The theorem is proved. □

Intuitively, the non-equivalence of mR and q-MLR should not be surprising given that entanglement in composite systems cannot be detected by independent measurements of the subsystems. Let us elaborate on this remark.

Remark 4.13. ρ in Theorem 4.8 is built up from d_ns where each d_n has r_n many entangled eigenvectors with non-zero eigenvalue and r_n many entangled eigenvectors with zero eigenvalue. This inhomogeneity in the distribution of eigenvalues is solely due to these entangled eigenvectors (all the $2^n - 2r_n$ many non entangled eigenvectors of d_n have the same non-zero eigenvalues). A crucial part in showing that ρ is non q-MLR was to use the inhomogeneous eigenvalue distribution to bound the size M_N (see 4.6 in the proof of Lemma 4.9). Heuristically speaking, the the non-quantum randomness of ρ is a reflection of the non-uniform eigenvalue distribution of d_n which in turn is due to the presence of entangled eigenvectors of d_n. It is hence reasonable to expect that the quantum non-randomness of ρ, which stems from entanglement, cannot be captured by measurements in the sense of Definition 4.2 using pure tensors (i.e. measuring each 2-dimensional subsystem independently).

4.5 Generalizations

We sketch some ways in which the Section 4.4's results generalize. Given $S \in 2^\omega$, we may relativize the notion of Martin-Löf randomness to define the set $MLR^S \subset 2^\omega$ of infinite bitstrings which are Martin-Löf random with respect to S. The halting problem, denoted by $\varnothing' \subset \mathbb{N}$ is an incomputable set important in computability theory. Letting $\varnothing^{(n)}$ be the $n-1$th iterate of the halting problem, an element of Cantor space is said to

be *arithmetically random* if it is in $MLR^{\varnothing^{(n)}}$ for every n (see 6.8.4 in [21]). Given $S \in 2^\omega$, relativizing the proof of Lemma 4.12 shows that $MLR^S(\mu_\rho^B) \subseteq MLR^S$ as follows. Take an $X \in MLR^S(\mu_\rho^B)$. Relativizing Theorems 85 and 90 from [22] and 3.2.14 from [28] to S and noting that $KM^S(.) \leqslant KM(.)$ and following the proof of Lemma 4.12 shows that $X \in MLR^S$. This shows that $\mu_\rho^B(MLR^S) = 1$ holds for any $S \in 2^\omega$ and any computable measurement system B. In particular, if B is any computable measurement system, $\mu_\rho^B(MLR^{\varnothing^{(n)}}) = 1$ for all n. So,

$$\mu_\rho^B\big[\bigcap_{n\in\mathbb{N}}(MLR^{\varnothing^{(n)}})\big] = 1.$$

So, measuring ρ, the state constructed in Theorem 4.8 in any computable measurement system yields an arithmetically random infinite sequence of bits, with probability one. The above note naturally suggests a definition:

Definition 4.14. ρ is said to be strong measurement random (strong mR), if $\mu_\rho^B(MLR^S) = 1$ holds for any $S \in 2^\omega$ and any computable measurement system B.

By Remark 4.4 and by the above discussion on relativizations, we can also consider measurement of a state in non-computable measurement systems by using an appropriate oracle. We do not explore this here.

One may ask if we can build other computable examples of ρs which are not q-MLR and are mR. We note that a straightforward modification of the proof of Theorem 4.8 yields a family of such ρs. We do not provide all the details here for lack of space. Let $h : \mathbb{N} \longrightarrow \mathbb{N}$ and $g : \mathbb{N} \longrightarrow (0, 1)$ be computable, satisfying the following for some constants $\delta \in (0, 1)$ and $F > 0$:

$$\prod_{n=5}^{\infty}(1 - h(n)2^{-n}) = 0, \prod_{n=5}^{\infty}(1 - h(n)[2^{-n} - g(n)]) = \delta,$$

$$\forall n, g(n) \leqslant 2^{-n} \text{ and } \prod_{n=5}^{\infty} \big[1 - \frac{4g^2(n)h^2(n)}{(1-2g(n)h(n))^2}\big] = F.$$

Let ρ be defined as in the proof of the main Theorem but with r_n replaced by $h(n)$ and with the $h(n)$ many entries on the extreme ends of the anti-diagonal of d_n being equal to $g(n)$ instead of 2^{-n}. Then, this ρ is computable and mR (in fact, it is strong mR) and fails a q-MLT at order δ.

4.6 Measurement randomness and q-MLR for product states

Although Theorem 4.8 shows that mR and q-MLR are not equivalent in general, it is interesting to investigate if these notions are indeed equivalent for certain special states.

Definition 4.15. A state $\rho = (\rho_s)_s$ is defined to be a product state if there is a 2^m by 2^m computable density matrix d such that for all n, $\rho_{nm} = \otimes_{s=1}^{n} d$.

Theorem 4.16. Measurement randomness is equivalent to q-MLR for product states.

We first prove some purely linear algebraic lemmas. We will use the block matrix and block vector notation; capital letters will indicate that the block is a matrix and not a scalar. For $n \geqslant 1$, unit vector $v \in \mathbb{C}^{2^n}$ will be called *atomic* if it is of the form $v = \otimes_{s=1}^{n} v_s$ for some complex algebraic unit vectors $v_s \in \mathbb{C}^2$. I.e., $v \in \mathbb{C}^{2^n}$ is atomic if it is a product tensor of n many complex algebraic unit vectors, $v_s \in \mathbb{C}^2$.

Lemma 4.17. If E is 2^n by 2^n and $v^\dagger E v = 0$ for all atomic $v \in \mathbb{C}^{2^n}$, then E is the zero matrix.

Proof. The proof is by induction. Suppose E is 2^{n+1} by 2^{n+1} and satisfies the hypotheses of the lemma. Let

$$E = \begin{bmatrix} A & B \\ C & D \end{bmatrix},$$

where each block is 2^n by 2^n. Let X be an arbitrary 2^n by 1, atomic column vector. Then, if $\overline{0}$ represents the 2^n by 1 zero column vector,

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes X = \begin{bmatrix} X \\ \overline{0} \end{bmatrix}$$

is atomic too. So,

$$\begin{bmatrix} X^\dagger & \overline{0} \end{bmatrix} \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} X \\ \overline{0} \end{bmatrix} = X^\dagger A X = 0.$$

As X was an arbitrary atomic vector, A is the zero matrix by the induction hypothesis. Similarly, D is the zero matrix. Note that

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \otimes X = \frac{1}{\sqrt{2}} \begin{bmatrix} X \\ X \end{bmatrix}$$

is atomic. So,

$$0 = \frac{1}{\sqrt{2}} \begin{bmatrix} X^\dagger & X^\dagger \end{bmatrix} E \frac{1}{\sqrt{2}} \begin{bmatrix} X \\ X \end{bmatrix} = \begin{bmatrix} X^\dagger & X^\dagger \end{bmatrix} \begin{bmatrix} 0 & B/2 \\ C/2 & 0 \end{bmatrix} \begin{bmatrix} X \\ X \end{bmatrix} = \frac{(X^\dagger B X + X^\dagger C X)}{2}.$$

So, for all atomic X, $X^\dagger(B + C)X = 0$. By the induction hypothesis, $B = -C$.

$$\begin{bmatrix} \frac{i}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} \otimes X = \begin{bmatrix} \frac{i}{2} X \\ \frac{\sqrt{3}}{2} X \end{bmatrix}$$

is atomic. So,

$$0 = \begin{bmatrix} \frac{-i}{2} X^\dagger & \frac{\sqrt{3}}{2} X^\dagger \end{bmatrix} E \begin{bmatrix} \frac{i}{2} X \\ \frac{\sqrt{3}}{2} X \end{bmatrix} = \begin{bmatrix} \frac{-i}{2} X^\dagger & \frac{\sqrt{3}}{2} X^\dagger \end{bmatrix} \begin{bmatrix} 0 & -B \\ B & 0 \end{bmatrix} \begin{bmatrix} \frac{i}{2} X \\ \frac{\sqrt{3}}{2} X \end{bmatrix} = \frac{i\sqrt{3}}{2} X^\dagger B X.$$

So, for all atomic X, $X^\dagger BX = 0$. By the induction hypothesis, $B = 0$. This proves the induction step. We omit the details of the base case (i.e., when $n = 1$ and E is two by two) as it can be proved similarly to the induction step. □

Let I_n denote the 2^n by 2^n identity matrix.

Lemma 4.18. If E is a 2^n by 2^n Hermitian matrix such that $v^\dagger Ev = 2^{-n}$ for all atomic $v \in \mathbb{C}^{2^n}$, then $E = 2^{-n} I_n$.

Proof. The proof is by induction. Suppose E is 2^{n+1} by 2^{n+1} and satisfies the hypotheses of the lemma. Note that because the standard (computational) basis vectors are atomic, E has 2^{-n-1} along the diagonal. Let

$$E = \begin{bmatrix} A & B \\ B^\dagger & C \end{bmatrix},$$

where each block is 2^n by 2^n. Let X be an arbitrary 2^n by 1, atomic column vector. Then, if $\overline{0}$ represents the 2^n by 1 zero column vector,

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes X = \begin{bmatrix} X \\ \overline{0} \end{bmatrix}$$

is atomic too. So,

$$\begin{bmatrix} X^\dagger & \overline{0} \end{bmatrix} \begin{bmatrix} A & B \\ B^\dagger & C \end{bmatrix} \begin{bmatrix} X \\ \overline{0} \end{bmatrix} = X^\dagger AX = 2^{-n-1}.$$

So, for an arbitrary atomic vector X ,

$$X^\dagger (2A) X = 2^{-n}.$$

Note that $2A = 2A^\dagger$ (as $E = E^\dagger$) and that $2A$ has 2^{-n} along the diagonal. So, by the induction hypothesis, $2A = 2^{-n} I_n$. Similarly, $2C = 2^{-n} I_n$.

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \otimes X = \frac{1}{\sqrt{2}} \begin{bmatrix} X \\ X \end{bmatrix}$$

is atomic. So,

$$2^{-n-1} = \frac{1}{\sqrt{2}} \begin{bmatrix} X^\dagger & X^\dagger \end{bmatrix} E \frac{1}{\sqrt{2}} \begin{bmatrix} X \\ X \end{bmatrix} = \begin{bmatrix} X^\dagger & X^\dagger \end{bmatrix} \begin{bmatrix} 2^{-n-2} I_n & B/2 \\ B^\dagger/2 & 2^{-n-2} I_n \end{bmatrix} \begin{bmatrix} X \\ X \end{bmatrix}$$

$$= \frac{(X^\dagger B X + X^\dagger B^\dagger X)}{2} + 2^{-n-1}.$$

So, for all atomic X, $\mathrm{Re}(X^\dagger B X) = 0$. Similarly, we show that $\mathrm{Im}(X^\dagger B X) = 0$ as follows:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{bmatrix} \otimes X = \frac{1}{\sqrt{2}} \begin{bmatrix} X \\ iX \end{bmatrix}$$

is atomic. So,

$$2^{-n-1} = \frac{1}{\sqrt{2}} \begin{bmatrix} X^\dagger & -iX^\dagger \end{bmatrix} E \frac{1}{\sqrt{2}} \begin{bmatrix} X \\ iX \end{bmatrix}$$

$$= \begin{bmatrix} X^\dagger & -iX^\dagger \end{bmatrix} \begin{bmatrix} 2^{-n-2} I_n & B/2 \\ B^\dagger/2 & 2^{-n-2} I_n \end{bmatrix} \begin{bmatrix} X \\ iX \end{bmatrix} = \frac{i(X^\dagger B X - X^\dagger B^\dagger X)}{2} + 2^{-n-1}.$$

So, for all atomic X, $X^\dagger B X = 0$. By Lemma 4.17, B is the zero matrix. This proves the induction step. We omit the details of the base case (i.e., when $n = 1$ and E is Hermitian two by two) as it can be proved similarly to the induction step. □

We now prove Theorem 4.16.

Proof. By Theorem 4.6, it suffices to show that if a product state ρ is mR, then it is q-MLR. Let state $\rho = (\rho_s)_s$ be a mR product state. So, there is a 2^m by 2^m computable density matrix d such that for all n, $\rho_{nm} = \otimes_{s=1}^{n} d$. We show, using Lemma 4.18, that d must be the $2^{-n} I_n$, and hence that ρ is q-MLR. Suppose that there is an atomic $v \in C^{2^n}$ and a p such that $v^\dagger d v = p \neq 2^{-n}$ (Note that $p \in [0,1]$ as d is a density matrix). So, $v = \otimes_{s=1}^{n} v_s$ for some complex algebraic unit vectors $v_s \in \mathbb{C}^2$. For each s, let w_s be the unique complex algebraic unit vector such that v_s and w_s form a orthonormal basis of $\mathbb{C}^2$. Define a measurement system by $B = ((b_0^t, b_1^t))_{t=1}^{\infty}$ where $b_0^t := v_s$ and $b_1^t := w_s$ for $t = s \pmod n$. I.e., informally speaking, B consists of copies of v. As v has 'length' equal to n, B repeats with period n. Consider dividing an infinite bitstring, X into blocks of length n (I.e., the first block is $X(1)X(2)\cdots X(n)$, the second block is $X(n+1)X(n+2)\cdots X(2n)$ and so on). Given an X, let $f_X(s) =$ the number of blocks which are equal to 0^n in the first sn many bits of X. By the strong law of large numbers, for μ_B^ρ- almost every X,

$$\lim_{s\to\infty} \frac{f_X(s)}{s} = p.$$

However, it is known that if X is MLR, then

$$\lim_{s\to\infty} \frac{f_X(s)}{s} = 2^{-n} \neq p.$$

So, $\mu_B^\rho(MLR) = 0$ and so ρ is not mR. So, such v and p cannot exist and by Lemma 4.18, $d = 2^{-n} I_n$. □

4.7 Conclusion

We constructed a computable, non-random qubitstring which almost surely yields a arithmetic random bitstring when measured. Formally, we construct a computable, non q-MLR state which yields an arithmetically random bitstring with probability one when 'measured'. Arithmetic randomness is a strong form of classical randomness, strictly stronger than Martin-Löf randomness (See 6.8.4 in [21] for details on arithmetic randomness). Our result hence provides further evidence for the philosophically and practically important claim that 'true' randomness (as against pseudorandomness) [15] can be extracted from certain quantum systems. While several schemes exist for generating a random bitstring from a quantum source [1, 3–5, 15, 25, 33], to the best of our knowledge, none of these produce arithmetic randomness. It hence seems plausible that our results may prove to be relevant to the construction of quantum random number generators [15, 23].

Abbott, Calude and Svozil have also studied bitstrings resulting from measuring a quantum system [1, 3]. However, their notion of measurement is significantly different from ours. In contrast to our work which considers measurement of an infinite sequence of qubits, they studied the randomness of a sequence of bits generated by *repeatedly measuring a finite dimensional* quantum system. They go on to apply this to quantum random number generators and their certification [1–3, 15].

4.8 Acknowledgements

I thank James Hanson for many helpful discussions pertaining to Section 4.6. Joe Miller and Peter Cholak (independently) asked if there is a notion of 'measuring a state'.

These questions were one of the factors which led me to explore this area. André Nies independently suggested that one might get a measure on Cantor space by 'measuring' a state.

Chapter 5

Entropy and computable states

The von Neumann entropy of a density matrix is the Shannon entropy of the distribution given by its eigenvalues [27]. In this chapter, we are concerned with the von Neumann entropies of the initial segments of states. Recall from Definition 1.7 that each finite initial segment τ_n of the tracial state τ is the maximally mixed state with a (maximum possible) von-Neumann entropy equal to n. This suggests that computable states whose initial segments' total eigenmass of one is 'evenly spread out' over all the eigenvalues are quantum Martin-Löf random (q-MLR). Heuristically speaking, since the eigenvectors of the initial segments of computable states are computable and hence easy to describe, the randomness of computable states cannot stem from the randomness of the individual eigenvectors of the initial segments. Rather, their randomness should result from the eigenvalue mass of their initial segments being 'uniformly spread out' and hence difficult to 'capture' using a quantum Martin-Löf test. The uniform spreading of the eigenvalues should be reflected in an asymptotically high von-Neumann entropy of the state (States having initial segments whose eigenvalues are evenly spread out have a 'high von-Neumann entropy', where we use the quotes as the von Neumann entropy is defined for density matrices and not for states. We describe below a way to make sense of von Neumann entropy for states).

Motivated by this, we explore the asymptotic behavior of the von-Neumann entropy

of the initial segments of computable states. Let $H(\rho_n)$ be the von-Neumann entropy of ρ_n. We show Theorems 5.4 and 5.2 which can be summarized as: For any computable ρ

$$\exists c\, \exists^\infty n\, H(\rho_n) > n - c \Rightarrow \rho \text{ is q-MLR} \Rightarrow H(\rho) := \lim_n \frac{H(\rho_n)}{n} = 1.$$

Further, we provide an example to show that the first implication does not reverse. It is easy to see that the second does not reverse too. So, these implications are strict.

Recall that weak Solovay randomness is equivalent to q-MLR for computable states and hence all results here also hold for weak Solovay random states.

Definition 5.1. The von-Neumann entropy $H(\rho_n)$ of a density matrix ρ_n on n qubits is defined as: Let ρ_n have a orthonormal eigenbasis $(|\psi^i\rangle)_{i\leqslant 2^n}$ and corresponding eigenvalues $(\alpha_i)_{i\leqslant 2^n}$. So,

$$\rho_n = \sum_{i\leqslant 2^n} \alpha_i |\psi^i\rangle\langle\psi^i|.$$

Since ρ is a density matrix, $Tr(\rho) = \sum_i \alpha_i = 1$. So, we can define:

$$H(\rho_n) = -\sum_{i\leqslant 2^n} \alpha_i \log_2(\alpha_i).$$

5.1 q-MLR implies maximum entropy per qubit.

Theorem 5.2 shows that, asymptotically speaking, computable q-MLR states have maximum von-Neumann entropy 'per qubit'.

Theorem 5.2. If $\rho = (\rho_n)_n$ is a computable quantum Martin-Löf random state, then

$$H(\rho) := \liminf_n \frac{H(\rho_n)}{n} = 1.$$

In fact, noting that for all n $\dfrac{H(\rho_n)}{n} \leqslant 1$ we have $\limsup_n \dfrac{H(\rho_n)}{n} \leqslant 1$. So, the theorem implies that $\lim_n \dfrac{H(\rho_n)}{n}$ exists and is 1.

Proof. Proof sketch: Suppose towards a contradiction that $H(\rho) < \epsilon < 1$. This implies that (see Lemma 5.3) there is a $\delta > 0$ such that for infinitely many n, there are $2^{n\epsilon}$ many eigenvalues $\alpha_1, ..., \alpha_{2^{n\epsilon}}$ of ρ_n with $\sum_i \alpha_i > \delta$. To prove this one argues as follows: If no such δ existed, then one can bound the entropies of the ρ_ns from below and show that $H(\rho) \geqslant \epsilon$. Then, the computability of ρ allows us to build a test which ρ fails at δ. Details: Towards a contradiction, let $\rho = (\rho_n)_n$ be q-MLR with $H(\rho) < \epsilon < 1$. Let

$$\rho_n = \sum_{i \leqslant 2^n} \alpha_i^n |\psi_i^n\rangle\langle\psi_i^n|,$$

where, $\alpha_1^n \geqslant \alpha_2^n \geqslant \cdots \geqslant \alpha_{2^n}^n$.

We begin with a lemma.

Lemma 5.3. For the above ϵ there is a $\delta > 0$ such that $\exists^\infty n$

$$\sum_{i \leqslant \lceil 2^{n\epsilon} \rceil} \alpha_i^n > \delta.$$

The lemma says that a constant (δ) amount of eigenvalue 'mass' concentrates at the first $\lceil 2^{n\epsilon} \rceil$ many largest eigenvalues, infinitely often.

Proof. Suppose towards a contradiction that $\forall \delta \, \exists N_\delta$ such that,

$$n > N_\delta \Rightarrow \sum_{i \leqslant \lceil 2^{n\epsilon} \rceil} \alpha_i^n \leqslant \delta.$$

Fix a $\delta < 0.5$ and a $n > N_\delta$. For this n, define the sequence $(r_i^n)_{i \leqslant 2^n}$ as follows: For $i < \lceil 2^{n\epsilon} \rceil$, let $r_i^n := \alpha_i^n$. For $\lceil 2^{n\epsilon} \rceil \leqslant i < I$ ($I \in \omega$ will be defined shortly), let $r_i^n := \alpha_{\lceil 2^{n\epsilon} \rceil}^n$. For $I \leqslant i \leqslant 2^n$, let $r_i^n := 0$. Here, I is picked to ensure that

$$1 - \alpha_{\lceil 2^{n\epsilon} \rceil}^n \leqslant \sum_{i \leqslant I} r_i^n \leqslant 1. \tag{5.1}$$

So, $r_i = \alpha_i$ from $1 \leqslant i \leqslant \lceil 2^{n\epsilon} \rceil$ and r_i is the constant $\alpha^n_{\lceil 2^{n\epsilon}\rceil}$ from $\lceil 2^{n\epsilon}\rceil \leqslant i < I$ where I is the largest number so that the r_i's sum to less than 1. Why does such an I exist? $\sum_{i<t} r^n_i$ increases by $\alpha^n_{\lceil 2^{n\epsilon}\rceil}$ when t increases by 1, for $t > \lceil 2^{n\epsilon}\rceil$. We can keep increasing t and stop the first time $\sum_{i<t} r^n_i > 1$. I.e., we find a I such that $\sum_{i\leqslant I} r^n_i < 1 \leqslant \sum_{i\leqslant I+1} r^n_i$. Since, $\sum_{i\leqslant I+1} r^n_i - \sum_{i\leqslant I} r^n_i = \alpha^n_{\lceil 2^{n\epsilon}\rceil}$, the inequality 5.1 holds. Let $S_n = \sum_i r^n_{i\leqslant 2^n}$ and we drop the subscript of S.

Let $p^n_i := S^{-1} r^n_i$. So, $p = (p^n_i)_{i\leqslant 2^n}$ is a probability distribution on 2^n and dominates $(r_i)_i$. Let $H(p)$ be its Shannon entropy, which we now bound from below.

$$H(p) = -\sum_{i<\lceil 2^{n\epsilon}\rceil} S^{-1}\alpha^n_i \log(S^{-1}\alpha^n_i) - \sum_{\lceil 2^{n\epsilon}\rceil \leqslant i\leqslant I} S^{-1}\alpha^n_{\lceil 2^{n\epsilon}\rceil}\log(S^{-1}\alpha^n_{\lceil 2^{n\epsilon}\rceil}).$$

$n > N_\delta$ implies that $\alpha^n_1 < \delta < 0.5$ and hence that for all i,

$$\alpha^n_i \leqslant \alpha^n_1 < \delta < 0.5. \tag{5.2}$$

Note that $0.5 < 1 - \delta$, since $\delta < 0.5$. So,

$$0.5 < 1 - \delta < 1 - \alpha^n_{\lceil 2^{n\epsilon}\rceil} \leqslant S \leqslant 1. \tag{5.3}$$

Putting 5.1, 5.2 and 5.3 together, for all i,

$$\alpha^n_i \leqslant \alpha^n_1 < \delta < 1 - \delta < 1 - \alpha^n_{\lceil 2^{n\epsilon}\rceil} \leqslant S \leqslant 1. \tag{5.4}$$

So, $\log(S^{-1}\alpha^n_i) \leqslant 0$ for all i. So, the first sum in the expression for $H(p)$ is non-negative. This gives,

$$H(p) > -\sum_{\lceil 2^{n\epsilon}\rceil \leqslant i\leqslant I} S^{-1}\alpha^n_{\lceil 2^{n\epsilon}\rceil}\log(S^{-1}\alpha^n_{\lceil 2^{n\epsilon}\rceil}) = -(I - \lceil 2^{n\epsilon}\rceil)S^{-1}\alpha^n_{\lceil 2^{n\epsilon}\rceil}\log(S^{-1}\alpha^n_{\lceil 2^{n\epsilon}\rceil}).$$

Again, since $\log(S^{-1}\alpha^n_{\lceil 2^{n\epsilon}\rceil}) < 0$, this sum is non-negative. So, we can ignore $S^{-1} \geqslant 1$ to get:

$$H(p) > -(I - \lceil 2^{n\epsilon}\rceil)\alpha^n_{\lceil 2^{n\epsilon}\rceil}\log(S^{-1}\alpha^n_{\lceil 2^{n\epsilon}\rceil}). \tag{5.5}$$

Now, by choice of $n > N_\delta$,

$$S = \sum_i r_i^n = \sum_{i<\lceil 2^{n\epsilon}\rceil} \alpha_i^n + (I - \lceil 2^{n\epsilon}\rceil)\alpha^n_{\lceil 2^{n\epsilon}\rceil} \leqslant \delta + (I - \lceil 2^{n\epsilon}\rceil)\alpha^n_{\lceil 2^{n\epsilon}\rceil}.$$

So,

$$S - \delta \leqslant (I - \lceil 2^{n\epsilon}\rceil)\alpha^n_{\lceil 2^{n\epsilon}\rceil}.$$

By the inequality 5.4,

$$1 - \delta \leqslant 1 - \alpha^n_{\lceil 2^{n\epsilon}\rceil} \leqslant S.$$

This gives,

$$1 - 2\delta \leqslant (I - \lceil 2^{n\epsilon}\rceil)\alpha^n_{\lceil 2^{n\epsilon}\rceil}.$$

Since, $-\log(S^{-1}\alpha^n_{\lceil 2^{n\epsilon}\rceil}) > 0$, we can put $1 - 2\delta$ in place of $(I - \lceil 2^{n\epsilon}\rceil)\alpha^n_{\lceil 2^{n\epsilon}\rceil}$ in 5.5 to get:

$$H(p) > -(1 - 2\delta)\log(S^{-1}\alpha^n_{\lceil 2^{n\epsilon}\rceil}). \tag{5.6}$$

Further, note that $\alpha^n_{\lceil 2^{n\epsilon}\rceil} \leqslant \delta 2^{-n\epsilon}$. (If not, then, for all $i \leqslant \lceil 2^{n\epsilon}\rceil$, $\alpha_i^n \geqslant \alpha^n_{\lceil 2^{n\epsilon}\rceil} > \delta 2^{-n\epsilon}$. This would give

$$\sum_{i\leqslant\lceil 2^{n\epsilon}\rceil} \alpha_i^n > \lceil 2^{-n\epsilon}\rceil 2^{-n\epsilon}\delta \geqslant 2^{n\epsilon}2^{-n\epsilon}\delta = \delta,$$

contradicting the choice of $n > N_\delta$). So, taking log on both sides:

$$\log(\alpha^n_{\lceil 2^{n\epsilon}\rceil}) \leqslant \log(\delta) + \log(2^{-n\epsilon}).$$

So,

$$-\log(\alpha^n_{\lceil 2^{n\epsilon}\rceil}) \geqslant -\log(\delta) + n\epsilon. \tag{5.7}$$

Using

$$-\log(S^{-1}\alpha^n_{\lceil 2^{n\epsilon}\rceil}) = \log(S) - \log(\alpha^n_{\lceil 2^{n\epsilon}\rceil}),$$

we can write inequality 5.6 as

$$H(p) > (1-2\delta)[\log(S) - \log(\alpha^n_{\lceil 2^{n\epsilon}\rceil})]. \tag{5.8}$$

Note that $\alpha = (\alpha^n_i)_i$ and $p = (p^n_i)_i$ are both distributions on 2^n with p dominating α on the support of p (Since $S \leqslant 1$, we have that $p_i > 0 \Rightarrow p_i = S^{-1}r_i \geqslant r_i \geqslant \alpha_i$) and α dominating p outside the support of p. So, by inequality 5.8, we have,

$$H(\rho_n) > (1-2\delta)[\log(S) - \log(\alpha^n_{\lceil 2^{n\epsilon}\rceil})]. \tag{5.9}$$

Recalling that $1-\delta < S \leqslant 1$ we have that $\log(S) > \log(1-\delta)$. By this and 5.7,

$$H(\rho_n) > (1-2\delta)[\log(1-\delta) - \log(\alpha^n_{\lceil 2^{n\epsilon}\rceil})] \geqslant (1-2\delta)[\log(1-\delta) - \log(\delta) + n\epsilon]. \tag{5.10}$$

So,

$$\frac{H(\rho_n)}{n} > (1-2\delta)\left[\frac{\log(1-\delta) - \log(\delta) + n\epsilon}{n}\right].$$

But this holds for any $n > N_\delta$ and so we have this inequality holding for each n in a sequence. So, using that $\liminf(x_n + y_n) \geqslant \liminf(x_n) + \liminf(y_n)$ we get:

$$H(\rho) = \liminf_n \frac{H(\rho_n)}{n} > (1-2\delta)\left[\liminf_n \frac{\log(1-\delta) - \log(\delta)}{n} + \epsilon\right] = (1-2\delta)\epsilon.$$

Recall that δ was arbitrary and so we have that for all δ, $H(\rho) > (1-2\delta)\epsilon$. By assumption, $H(\rho) < \epsilon$ and so we can find a δ_0 such that $H(\rho) < (1-2\delta_0)\epsilon < \epsilon$. Contradiction. □

Now, to get a contradiction, we build a q-MLT capturing ρ. Let δ be as in the previous lemma and without loss of generality, let δ be rational. Fix an m; we describe

the construction of $G^m = (G^m_n)_n$.

Find an n such that both of the following hold:

- $\sum_{i \leqslant \lceil 2^{n\epsilon} \rceil} \alpha^n_i > \delta$. (Infinitely many such n exist by the previous lemma.)
- $\dfrac{2^{n\epsilon}+1}{2^n} < 2^{-m}$. (This holds for almost every n since $\epsilon < 1$.)

Recall that ρ is computable and so the n can be found computably, uniformly in m. Set

$$G^m_n := \sum_{i \leqslant 2^{n\epsilon}} |\psi^i_n\rangle\langle\psi^i_n|.$$

For $k < n$, $G^m_k = \varnothing$ and for $k > n$, $G^m_k = G^m_n \otimes I^{k-n}$ where I is the 2-by-2 identity. Note that $2^{-n}Tr(G^m_n) < 2^{-m}$ by the second condition on n. Hence, $(G^m)_m$ is a q-MLT and $Tr(\rho_n G^m_n) > \delta$ by the first condition on n. So, ρ fails this test at δ. □

5.2 A condition on entropy which implies q-MLR.

Theorem 5.4 gives a condition on the von-Neumann entropy of a state which implies that it is q-MLR. The condition says that there is a fixed c such that ρ's von-Neumann entropy differs from that of the tracial state by at most c infinitely often. Recall that the tracial state is q-MLR. So, it is quite natural to expect that this condition implies q-MLR. Note that Theorem 5.4 holds for any state (not necessarily computable).

Theorem 5.4. Let $\rho = (\rho_n)_n$ be any state such that $\exists c\, \exists^\infty n\, H(\rho_n) > n - c$. Then, ρ is q-MLR.

Before proving this, recall the following consequence of the singular value decomposition (SVD).

Theorem 5.5. Let A be a n by d matrix with singular vectors $v_1, v_2, \ldots v_r$ and corresponding singular values $\sigma_1 \geqslant \sigma_2 \geqslant \cdots \geqslant \sigma_r$. Let $k \leqslant r$ and $w_1, w_2, \ldots, w_k$ be any orthonormal set. Then,

$$\sum_{i \leqslant k} |Av_i|^2 \geqslant \sum_{i \leqslant k} |Aw_i|^2.$$

For $\rho = \rho_n$ as above with eigenvalues (equal to the singular values since ρ is symmetric and positive semidefinite) $\alpha_1 \geqslant \alpha_2 \geqslant \cdots \geqslant \alpha_{2^n}$, let

$$\sqrt{\rho} = \sum_{i \leqslant 2^n} \sqrt{\alpha}_i |\psi^i\rangle\langle\psi^i|.$$

Note that $\sqrt{\rho}$ has eigenpairs $(\psi_i, \sqrt{\alpha}_i)$ and is positive semidefinite and symmetric. So, its eigenpairs are the same as its singular vector-singular value pairs. If $k \leqslant 2^n$ and $w_1, w_2, \ldots, w_k$ is any orthonormal set, then since the first k singular vectors of $\sqrt{\rho}$ are $\psi_1, \ldots, \psi_k$, Theorem 5.5 gives:

$$\sum_{i \leqslant k} |\sqrt{\rho}\psi_i|^2 \geqslant \sum_{i \leqslant k} |\sqrt{\rho}w_i|^2. \tag{5.11}$$

Let P be the orthogonal projection onto the subspace spanned by $w_1, w_2, \ldots, w_k$. Since $\sqrt{\rho}$ is self-adjoint, $\langle x|\sqrt{\rho}y\rangle = \langle(\sqrt{\rho})^* x|y\rangle = \langle\sqrt{\rho}x|y\rangle$. So,

$$Tr(\rho P) = \sum_{i \leqslant k} Tr(\rho|w_i\rangle\langle w_i|) = \sum_{i \leqslant k} \langle w_i|\rho|w_i\rangle = \sum_{i \leqslant k} \langle\sqrt{\rho}w_i|\sqrt{\rho}w_i\rangle = \sum_{i \leqslant k} |\sqrt{\rho}w_i|^2.$$

Similarly, if G is the orthogonal projection onto the subspace spanned by $\psi_1, \ldots, \psi_k$, then

$$Tr(\rho G) = \sum_{i \leqslant k} |\sqrt{\rho}\psi_i|^2.$$

So, by 5.11, for any rank k orthonormal projection, G, if P is the orthogonal projection onto the subspace spanned by the first k singular vectors of ρ, $\psi_1, \ldots, \psi_k$, then

$$Tr(\rho G) \leqslant Tr(\rho P) = \sum_{i \leqslant k} Tr(\rho|\psi_i\rangle\langle\psi_i|) = \sum_{i \leqslant k} \alpha_i. \tag{5.12}$$

Now we can prove Theorem 5.4.

Proof. Proof sketch: Suppose for a contradiction that ρ fails a q-MLT $(G_m)_m$ at δ. Fix an m. As ρ fails $(G_m)_m$ at δ we have that for a.e. n, the sum S_n of the first 2^{n-m} many largest eigenvalues of ρ_n exceeds δ. This implies that for a.e. n, $H(\rho_n) \leqslant 1-mS_n+n < 1-m\delta+n$ (to get this bound, we consider a distribution more 'uniform' than that induced by ρ_n and use its entropy to bound $H(\rho_n)$). Noting that m was arbitrary, we get a contradiction. Proof details: For a contradiction, let ρ satisfy the condition but not be q-MLR. Fix a q-MLT, $(G^m)_m$ and a $\delta > 0$ such that $\rho(G^m) > \delta$ for all m. I.e., $\forall m$ for almost every n, we have that $\mathrm{Tr}(\rho_n G^m_n) > \delta$. Note that since $\mathrm{rank}(G^m_n) \leqslant 2^{n-m}$, G^m_n is a orthogonal projection onto a subspace spanned by atmost 2^{n-m} orthonormal vectors. So, by 5.12, we have that for all m for a.e. n,

$$\delta < Tr(\rho_n G^m_n) \leqslant \sum_{i \leqslant 2^{n-m}} \alpha^n_i. \tag{5.13}$$

For a fixed m take a N_m such that for all $n > N_m$, 5.13 holds. For an $n > N_m$, let

$$S_{m,n} = \sum_{i \leqslant 2^{n-m}} \alpha^n_i.$$

Let $(r^m_n(i))_{i \leqslant 2^n}$ be the distribution on $1, 2, ..., 2^n$ defined by:

$r(i) = S_{m,n} 2^{m-n}$ if $i \leqslant 2^{n-m}$,

$r(i) = \dfrac{(1 - S_{m,n})}{2^n(1 - 2^{-m})}$ if $2^{n-m} < i \leqslant 2^n$.

The distribution $(r^m_n(i))_{i \leqslant 2^n}$ is uniform on each of the two intervals $\{1, ..., 2^{n-m}\}$ and $\{2^{n-m} + 1, ..., 2^n\}$. Its total mass on the first interval is $S_{m,n}$ and that on the second is $1 - S_{m,n}$. It is obtained by first considering the total mass of $(\alpha_n(i))_{i \leqslant 2^n}$ on each interval and then by uniformly distributing the mass within each interval. The distribution of the total mass between the 2 intervals is same for both $(r^m_n(i))_{i \leqslant 2^n}$ and $(\alpha_n(i))_{i \leqslant 2^n}$. Within each interval, $(r^m_n(i))_{i \leqslant 2^n}$ is at least as uniform as $(\alpha_n(i))_{i \leqslant 2^n}$. So, by Exercise 2.18 on

page 50 of the book by Thomas and Cover [18], we have that,

$$H(\rho_n) \leqslant H((r_n^m(i))_{i\leqslant 2^n}). \tag{5.14}$$

Recall that this holds for $\forall m$ and $\forall n > N_m$. Let, $(r_n^m(i))_{i\leqslant 2^n}$ be denoted by r_n^m. We now bound $H(r_n^m)$ from above to get a contradiction.

$$H(r_n^m) = -\left[2^{n-m}(S_{m,n}2^{m-n}\log(S_{m,n}2^{m-n}))+(2^n-2^{n-m})\frac{1-S_{m,n}}{2^n(1-2^{-m})}\log\left(\frac{1-S_{m,n}}{2^n(1-2^{-m})}\right)\right].$$

This simplifies to:

$$H(r_n^m) = h(S_{m,n}) - mS_{m,n} + n + (1-S_{m,n})\log(1-2^{-m}).$$

where $h(S_{m,n}) = -S_{m,n}\log(S_{m,n}) - (1-S_{m,n})\log(1-S_{m,n})$ is a positive real number between 0 and 1 and so we can replace it by 1 to get an upper bound. Note that $(1-S_{m,n})\log(1-2^{-m}) < 0$. So, we can drop it to get an upper bound,

$$H(r_n^m) \leqslant 1 - mS_{m,n} + n. \tag{5.15}$$

By 5.14 and 5.15, we get that for all m and for all $n > N_m$,

$$H(\rho_n) \leqslant H(r_n^m) \leqslant 1 - mS_{m,n} + n. \tag{5.16}$$

By assumption fix a c such that

$$\exists^\infty n, H(\rho_n) \geqslant n - c. \tag{5.17}$$

Now, for all m, 5.16 holds for almost every n and 5.17 holds for infinitely many n. So, for all m, 5.16 and 5.17 hold for infinitely many n. I.e.,

$$\forall m \exists^\infty n, \text{ such that } n - c \leqslant H(\rho_n) \leqslant 1 - mS_{m,n} + n.$$

So,

$$\forall m \exists^{\infty} n, \text{ such that } -c \leqslant 1 - mS_{m,n}.$$

So,

$$\forall m \exists^{\infty} n, \text{ such that } c \geqslant -1 + mS_{m,n}.$$

Noting that $S_{m,n} > \delta$ for $n > N_m$, we get that

$$\forall m \exists^{\infty} n, \text{ such that } c \geqslant -1 + mS_{m,n} \geqslant -1 + m\delta.$$

So, $\forall m, c + 1 \geqslant m\delta$. Contradiction. □

Remark 5.6. Any state differing from the tracial state at only finitely many qubits clearly satisfies the hypothesis of Theorem 5.4. We construct another one: Let f be any function on $(0, 1)$ satisfying

$$\int_0^1 f(s)ds = 1 \text{ and } -\infty < -\int_0^1 f(s) \log(f(s))ds < \infty.$$

For example, let

$$f(x) = \frac{2}{x(1 - \ln x)^3},$$

on $(0, 1)$ where ln stands for the natural logarithm. Define a diagonal state $\rho = (\rho_n)_n$ as follows. Fix n. For all $\sigma \in 2^n$ let

$$\alpha_\sigma = \int_{[\sigma]} f(s)ds.$$

Here, $[\sigma] \subset (0, 1]$ is the open interval defined by the string σ.

$$\rho_n = \sum_{\sigma \in 2^n} \alpha_\sigma |\sigma\rangle\langle\sigma|.$$

Note that ρ is coherent since $\alpha_\sigma = \alpha_{\sigma 1} + \alpha_{\sigma 0}$ by definition and since $\int_0^1 f(s)ds = 1$. Now we show that ρ satisfies the hypothesis of Theorem 5.4. For any n by definition of the α's, we have,

$$H(\rho_n) = -\sum_{\sigma \in 2^n} \int_{[\sigma]} f(s)ds \log\left(\int_{[\sigma]} f(s)ds\right).$$

By the mean-value theorem and continuity of f, for all σ there is a $x_\sigma \in [\sigma]$ such that

$$\int_{[\sigma]} f(s)ds = 2^{-n} f(x_\sigma).$$

So

$$\begin{aligned} H(\rho_n) &= -\sum_{\sigma \in 2^n} 2^{-n} f(x_\sigma) \log(2^{-n} f(x_\sigma)) \\ &= -\sum_{\sigma \in 2^n} 2^{-n} f(x_\sigma)(-n + \log(f(x_\sigma))) \\ &= -\sum_{\sigma \in 2^n} 2^{-n} f(x_\sigma)\log(f(x_\sigma)) + n \sum_{\sigma \in 2^n} 2^{-n} f(x_\sigma) \\ &= -\sum_{\sigma \in 2^n} 2^{-n} f(x_\sigma)\log(f(x_\sigma)) + n \sum_{\sigma \in 2^n} \int_{[\sigma]} f(s)ds \\ &= \text{Riemann Sum}[-f(.)\log(f(.)), \text{Mesh Size} = 2^{-n}] + n \int_0^1 f(s)ds. \end{aligned}$$

So, as the last integral is equal to 1,

$$H(\rho_n) - n = \text{Riemann Sum}[-f(.)\log(f(.)), \text{Mesh Size} = 2^{-n}].$$

But,$-\int_0^1 f(s)\log(f(s))ds = c$, for some constant c. Since the Reimann Sum converges to c, we have that $H(\rho_n) - n = O(1)$ as required.

We now give an example to show that Theorem 5.4 cannot be reversed. The construction will be along the same lines as the preceding remark. Let f be any function on $(0, 1)$ satisfying:

$$\int_0^1 f(s)ds = 1 \text{ and } -\int_0^1 f(s)\log(f(s))ds = -\infty.$$

For example, let

$$f(x) = \frac{1}{x(1-\ln x)^2}$$

on $(0,1)$. Define a diagonal state $\rho = (\rho_n)_n$ as follows. Fix n. For all $\sigma \in 2^n$ let

$$\alpha_\sigma = \int_{[\sigma]} f(s)ds.$$

Here, $[\sigma] \subset (0,1]$ is the open interval defined by the string σ. We let

$$\rho_n = \sum_{\sigma \in 2^n} \alpha_\sigma |\sigma\rangle\langle\sigma|.$$

Note that ρ is coherent since $\alpha_\sigma = \alpha_{\sigma 1} + \alpha_{\sigma 0}$ by definition.

Lemma 5.7. ρ is q-MLR.

Proof. Let $(G^m)_m$ be the universal q-MLT. Given a $\delta > 0$ we find an m such that $\rho(G^m) < \delta$. Since f is in $L_1[0,1]$, by absolute continuity, find a m such that

$$\int_I f(s)ds < \delta,$$

for any interval $I \subset (0,1)$, with $|I| \leqslant 2^{-m}$. We claim that this m works by showing that for all n, $Tr(\rho_n G_n^m) < \delta$. Fix an n. G_n^m is an orthogonal projection with rank at most 2^{n-m}. By using the consequence of the singular value decomposition,

$$Tr(\rho_n G_n^m) < \sum_{\sigma \in L} \alpha_\sigma = \sum_{\sigma \in L} \int_{[\sigma]} f(s)ds = \int_E f(s)ds < \delta,$$

where L is the set of σ's corresponding to the 2^{n-m} largest singular values of ρ_n, which are the α_σ's. I.e., L $= \{\sigma_1, ...\sigma_{2^{n-m}}\}$ if $\{\alpha_{\sigma_1}, ...\alpha_{\sigma_{2^{n-m}}}\}$ are the first 2^{n-m} largest α's. $E = \bigcup_L [\sigma]$ is a interval. Since $|L| = 2^{n-m}$ and $|[\sigma]| = 2^{-n}$, we have that $|E| = 2^{-n}2^{n-m} = 2^{-m}$. □

Lemma 5.8. For all $c > 0$, for almost every n, $H(\rho_n) - n < -c$. So, the condition of Theorem 5.4 does not hold for ρ.

Proof. For any n, by definition of the α's, we have,

$$H(\rho_n) = -\sum_{\sigma\in 2^n} \int_{[\sigma]} f(s)ds \log\Big(\int_{[\sigma]} f(s)ds\Big).$$

By the mean-value theorem and continuity of f for all σ there is a $x_\sigma \in [\sigma]$ such that

$$\int_{[\sigma]} f(s)ds = 2^{-n} f(x_\sigma).$$

So,

$$\begin{aligned} H(\rho_n) &= -\sum_{\sigma\in 2^n} 2^{-n} f(x_\sigma)\log(2^{-n} f(x_\sigma)) \\ &= -\sum_{\sigma\in 2^n} 2^{-n} f(x_\sigma)(-n + \log(f(x_\sigma))) \\ &= -\sum_{\sigma\in 2^n} 2^{-n} f(x_\sigma)\log(f(x_\sigma)) + n\sum_{\sigma\in 2^n} 2^{-n} f(x_\sigma) \\ &= -\sum_{\sigma\in 2^n} 2^{-n} f(x_\sigma)\log(f(x_\sigma)) + n\sum_{\sigma\in 2^n} \int_{[\sigma]} f(s)ds \\ &= \text{Riemann Sum}[-f(.)\log(f(.), \text{Mesh Size} = 2^{-n}] + n\int_0^1 f(s)ds. \end{aligned}$$

So, as the last integral is equal to 1,

$$H(\rho_n) - n = \text{Riemann Sum}[-f(.)\log(f(.), \text{Mesh Size} = 2^{-n}].$$

But, $-\int_0^1 f(s)\log(f(s))ds = -\infty$. So,

$$\begin{aligned} \lim_{n\to\infty} H(\rho_n) - n &= \lim_{n\to\infty} \text{Riemann Sum}[-f(.)\log(f(.), \text{Mesh Size} = 2^{-n}] \\ &= -\int_0^1 f(s)\log(f(s)ds = -\infty. \end{aligned}$$

So, for all $c \in \omega$ there is an N such that $n > N$ implies that $H(\rho_n) - n < -c$. □

So, ρ is the required computable q-MLR.

Chapter 6

Open questions

An important open question is whether weak Solovay random states have a Levin–Schnorr characterization in terms of QK. Techniques similar to those used in Subsection 3.3.3 may prove to be useful in answering this.

It still remains to find a complexity based characterization of q-MLR states. In this direction, Nies and Scholz found a partial Miller–Yu theorem concerning the quantum descriptive complexity of q-MLR and weak Solovay random states [31]. One can ask whether a Miller–Yu type result holds for q-MLR and/or weak Solovay random states when using QK as a complexity measure.

An interesting question is whether weak Solovay randomness is equivalent to q-MLR, a positive answer to which will yield a QK based characterizations (namely, those in Theorems 3.11 and 3.13) of q-MLR.

Another interesting question is to find a von-Neumann entropy based characterization of q-MLR for computable states. Chapter 5 contains partial results towards answering this question.

Bibliography

[1] A. A. Abbott, *Value Indefiniteness, Randomness and Unpredictability in Quantum Foundations. (De la Valeur Indéfinie aux Notions d'Aléatoire et d'Imprévisibilité Quantiques)*, PhD thesis, École Normale Supérieure, Paris, France, 2015.

[2] A. A. Abbott, C. S. Calude, and K. Svozil, *A quantum random number generator certified by value indefiniteness*, Mathematical Structures in Computer Science, 24 (2014).

[3] ——, *On the unpredictability of individual quantum measurement outcomes*, in Fields of Logic and Computation II, vol. 9300 of Lecture Notes in Computer Science, Springer, 2015, pp. 69–86.

[4] J. M. Agüero Trejo and C. S. Calude, *New quantum random number generators certified by value indefiniteness*, Theoretical Computer Science, (2020).

[5] Ä. Baumeler, C. Bedard, G. Brassard, and S. Wolf, *Kolmogorov amplification from Bell correlation*, 2017 IEEE International Symposium on Information Theory (ISIT), (2017), pp. 1544–1558.

[6] F. Benatti, T. Krüger, M. Müller, R. Siegmund-Schultze, and A. Szkola, *Entropy and quantum Kolmogorov complexity: A quantum Brudno's theorem*, Communications in Mathematical Physics, 265 (2006), pp. 437–461.

[7] E. Bernstein and U. Vazirani, *Quantum complexity theory*, SIAM Journal on Computing, 26 (1997), pp. 1411–1473.

[8] A. Berthiaume, W. van Dam, and S. Laplante, *Quantum Kolmogorov complexity*, J. Comput. Syst. Sci., 63 (2001), pp. 201–221.

[9] T. Bhojraj, *Generating randomness from a computable, non-random sequence of qubits*, Electronic Proceedings in Theoretical Computer Science, 318 (2020), p. 1–12.

[10] T. Bhojraj, *Prefix-free quantum Kolmogorov complexity*, Theoretical Computer Science, 875 (2021), pp. 65–80.

[11] T. Bhojraj, *Quantum algorithmic randomness*, Journal of Mathematical Physics, 62 (2021), p. 022202.

[12] I. Bjelakovic, T. Krüger, R. Siegmund-Schultze, and A. Szkola, *The Shannon-McMillan theorem for ergodic quantum lattice systems*, Inventiones mathematicae, 155 (2002).

[13] A. Bracken, *Entangled subspaces and quantum symmetries*, Physical Review A, 69 (2003).

[14] C. S. Calude, *Information and Randomness - An Algorithmic Perspective*, Texts in Theoretical Computer Science. An EATCS Series, Springer, 2002.

[15] ——, *Quantum randomness: From practice to theory and back*, in The Incomputable: Journeys Beyond the Turing Barrier, S. B. Cooper and M. I. Soskova, eds., Theory and Applications of Computability, Springer International Publishing, 2017, pp. 169–181.

[16] G. Chaitin, *Incompleteness theorems for random reals*, Adv. Appl. Math., 8 (1987), pp. 119–146.

[17] I. Chuang and M. Nielsen, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, second ed., 2000. ISBN-13: 978-1107002173.

[18] T. M. Cover and J. A. Thomas, *Elements of Information Theory 2nd Edition (Wiley Series in Telecommunications and Signal Processing)*, Wiley-Interscience, July 2006.

[19] M. Demianowicz and R. Augusiak, *Entanglement of genuinely entangled subspaces and states: exact, approximate, and numerical results*, eprint= 1907.12463, (2019).

[20] R. G. Downey and E. J. Griffiths, *Schnorr randomness*, The Journal of Symbolic Logic, 69 (2004), pp. 533–554.

[21] R. G. Downey and D. R. Hirschfeldt, *Algorithmic randomness and complexity*, Month 2010. 0387684417, 9780387684413.

[22] A. S. et al., *Kolmogorov Complexity and Algorithmic Randomness*, vol. : 220 of Mathematical Surveys and Monographs, AMS, 2017. ISBN: 978-1-4704-3182-2.

[23] M. Herrero-Collantes and J. C. Garcia-Escartin, *Quantum random number generators*, Rev. Mod. Phys., 89 (2017), p. 015004.

[24] M. Hoyrup, *The dimension of ergodic random sequences*, in 29th International Symposium on Theoretical Aspects of Computer Science (STACS 2012), C. Dürr and T. Wilke, eds., vol. 14 of Leibniz International Proceedings in Informatics

(LIPIcs), Dagstuhl, Germany, 2012, Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, pp. 567–576.

[25] M. Kessler and R. Arnon-Friedman, *Device-independent randomness amplification and privatization*, IEEE Journal on Selected Areas in Information Theory, 1 (2020), p. 568–584.

[26] M. Müller, *Quantum Kolmogorov complexity and the quantum Turing machine*, 2007.

[27] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, New York, NY, USA, 10th ed., 2011.

[28] A. Nies, *Computability and randomness*, Month 2009. ISBN: 0199230765, 9780199230761.

[29] A. Nies, *Logic blog 2017*, arXiv:1804.05331, (2017).

[30] A. Nies and V. Scholz, *Martin-Löf random quantum states*. arXiv:1709.08422v1, The first draft, September 2017.

[31] A. Nies and V. B. Scholz, *Martin-Löf random quantum states*, Journal of Mathematical Physics, 60 (2019), p. 092201.

[32] A. Nies and F. Stephan, *A weak randomness notion for probability measures*. arXiv:1902.07871, 2019.

[33] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning,

AND ET AL., *Random numbers certified by Bell's theorem*, Nature, 464 (2010), p. 1021–1024.

[34] P. A. REGALIA AND S. K. MITRA, *Kronecker products, unitary matrices, and signal processing applications*, SIAM Rev., 31 (1989), pp. 586–613.

[35] P. M. B. VITÁNYI, *Quantum Kolmogorov complexity based on classical descriptions*, ArXiv, quant-ph/0102108 (2001).