SCIS 2017 2017 Symposium on
Cryptography and Information Security
Naha, Japan, Jan. 24 - 27, 2017
The Institute of Electronics,
Information and Communication Engineers

A Refinement of Quantum Mechanics by Algorithmic Randomness and Its Application to Quantum Cryptography[*]

Kohtaro Tadaki [†]

Abstract: The notion of probability plays a crucial role in quantum mechanics. It appears in quantum mechanics as the Born rule. In modern mathematics which describes quantum mechanics, however, probability theory means nothing other than measure theory, and therefore any operational characterization of the notion of probability is still missing in quantum mechanics. We present an alternative rule to the Born rule based on the toolkit of *algorithmic randomness* by specifying the property of the results of quantum measurements in an operational way. Algorithmic randomness is a field of mathematics which enables us to consider the randomness of an individual infinite sequence. We then present an alternative rule to the Born rule for mixed states based on algorithmic randomness. In particular, we give a precise definition for the notion of mixed state. We then show that all of the alternative rules for both pure states and mixed states can be derived from a single postulate, called the *principle of typicality*, in a unified manner. We do this from the point of view of the *many-worlds interpretation of quantum mechanics.* Finally, we make an application of our framework to the BB84 quantum key distribution protocol in order to demonstrate how properly our framework works in a practical problem.

Keywords: quantum mechanics, Born rule, probability interpretation, algorithmic randomness, operational characterization, Martin-Löf randomness, many-worlds interpretation, the principle of typicality, quantum cryptography

1 Introduction

The notion of probability plays a crucial role in quantum mechanics. It appears in quantum mechanics as the so-called *Born rule*, i.e., *the probability interpretation of the wave function.* In modern mathematics which describes quantum mechanics, however, probability theory means nothing other than measure theory, and therefore any operational characterization of the notion of probability is still missing in quantum mechanics. In this sense, the current form of quantum mechanics is considered to be *imperfect* as a physical theory which must stand on operational means.

In a series of works [10, 11, 12], we presented an operational characterization of the notion of probability, based on the toolkit of *algorithmic randomness.* Algorithmic randomness, also known as *algorithmic information theory*, is a field of mathematics which enables us to consider the randomness of an *individual* infinite sequence. We used the notion of *Martin-Löf randomness with respect to Bernoulli measure* to present the operational characterization of the notion of probability. We gave natural and equivalent operational characterizations of the basic notions of probability theory, such as the notions of conditional probability and the independence of events/random variables, in terms of the notion of Martin-Löf randomness with respect to Bernoulli measure. We then made applications of our framework [10, 11, 12] to information theory and cryptography as examples of the fields for the applications, in order to demonstrate the wide applicability of our framework to the general areas of science and technology.

In this paper, as a major application of our framework [10, 11, 12] to basic science, we present an alternative rule to the Born rule based on our operational characterization of the notion of probability for the purpose of making quantum mechanics *perfect.* Namely, we use the notion of Martin-Löf randomness with respect to Bernoulli measure to state the alternative rule to the Born rule for specifying the property of the results of quantum measurements *in an operational way.*

As the first step of the research of this line, in the paper we only consider, for simplicity, the case of finite-dimensional quantum systems and measurements over them. Note, however, that *such a case is typical in quantum information and quantum computation.*

2 Mathematical Preliminaries

2.1 Basic Notation and Definitions

We start with some notation about numbers and strings which will be used in this paper.

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ is the set of *natural numbers*, and

[*] This work was partially supported by JSPS KAKENHI Grant Numbers 24540142, 15K04981. This work was partially done while the author was visiting the Institute for Mathematical Sciences, National University of Singapore in 2014.

[†] Department of Computer Science, College of Engineering, Chubu University, 1200 Matsumoto-cho, Kasugai-shi, Aichi 487-8501, Japan. E-mail: tadaki@cs.chubu.ac.jp WWW: http://www2.odn.ne.jp/tadaki/

$\mathbb{N}^+$ is the set of *positive integers*. $\mathbb{R}$ is the set of *reals*, and $\mathbb{C}$ is the set of *complex numbers*.

An *alphabet* is a non-empty finite set. Let Ω be an arbitrary alphabet throughout the rest of this section. A *finite string over* Ω is a finite sequence of elements from the alphabet Ω. We use Ω^* to denote the set of all finite strings over Ω, which contains the *empty string* denoted by λ. For any $\sigma \in \Omega^*$, $|\sigma|$ is the *length* of σ. Therefore $|\lambda| = 0$. For any $n \in \mathbb{N}$, we use Ω^n to denote the set $\{ x \mid x \in \Omega^* \ \&\ |x| = n\}$. A subset S of Ω^* is called *prefix-free* if no string in S is a prefix of another string in S.

An *infinite sequence over* Ω is an infinite sequence of elements from the alphabet Ω, where the sequence is infinite to the right but finite to the left. We use Ω^∞ to denote the set of all infinite sequences over Ω. Let $\alpha \in \Omega^\infty$. For any $n \in \mathbb{N}$, we denote by $\alpha\restriction_n \in \Omega^*$ the first n elements in the infinite sequence α. For any $S \subset \Omega^*$, the set $\{\alpha \in \Omega^\infty \mid \exists\, n \in \mathbb{N}\ \alpha\restriction_n \in S\}$ is denoted by $[S]^{\prec}$. For any $\sigma \in \Omega^*$, we denote by $[\sigma]^{\prec}$ the set $[\{\sigma\}]^{\prec}$.

2.2 Measure Theory

We briefly review measure theory according to Nies [8, Section 1.9].

A real-valued function μ defined on the class of all subsets of Ω^∞ is called an *outer measure on* Ω^∞ if the following conditions hold: (i) $\mu(\emptyset) = 0$; (ii) $\mu(\mathcal{C}) \le \mu(\mathcal{D})$ for every subsets $\mathcal{C}$ and $\mathcal{D}$ of Ω^∞ with $\mathcal{C} \subset \mathcal{D}$; (iii) $\mu\left(\bigcup_i \mathcal{C}_i\right) \le \sum_i \mu(\mathcal{C}_i)$ for every sequence $\{\mathcal{C}_i\}_{i\in\mathbb{N}}$ of subsets of Ω^∞. A *probability measure representation over* Ω is a function $r\colon \Omega^* \to [0,1]$ such that (i) $r(\lambda) = 1$ and (ii) for every $\sigma \in \Omega^*$ it holds that $r(\sigma) = \sum_{a\in\Omega} r(\sigma a)$. A probability measure representation r over Ω *induces* an outer measure μ_r on Ω^∞ in the following manner: A subset $\mathcal{R}$ of Ω^∞ is *open* if $\mathcal{R} = [S]^{\prec}$ for some $S \subset \Omega^*$. Let r be an arbitrary probability measure representation over Ω. For each open subset $\mathcal{A}$ of Ω^∞, we define $\mu_r(\mathcal{A})$ by $\mu_r(\mathcal{A}) := \sum_{\sigma\in E} r(\sigma)$, where E is a prefix-free subset of Ω^* with $[E]^{\prec} = \mathcal{A}$. Note that the sum is independent of the choice of the prefix-free set E and therefore the value $\mu_r(\mathcal{A})$ is well-defined. Then, for any subset $\mathcal{C}$ of Ω^∞, we define $\mu_r(\mathcal{C})$ as $\inf\{\mu_r(\mathcal{A}) \mid \mathcal{C} \subset \mathcal{A} \ \&\ \mathcal{A} \text{ is an open subset of } \Omega^\infty\}$. We can then show that μ_r is an *outer measure* on Ω^∞ such that $\mu_r(\Omega^\infty) = 1$.

A class $\mathcal{F}$ of subsets of Ω^∞ is called a *σ-field on* Ω^∞ if $\mathcal{F}$ includes Ω^∞, is closed under complements, and is closed under the formation of countable unions. The *Borel class* $\mathcal{B}_\Omega$ is the σ-field *generated by* all open sets on Ω^∞. Namely, $\mathcal{B}_\Omega$ is defined as the intersection of all the σ-fields on Ω^∞ containing all open sets on Ω^∞. A real-valued function μ defined on the Borel class $\mathcal{B}_\Omega$ is called a *probability measure on* Ω^∞ if the following conditions hold: (i) $\mu(\emptyset) = 0$ and $\mu(\Omega^\infty) = 1$; (ii) $\mu\left(\bigcup_i \mathcal{D}_i\right) = \sum_i \mu(\mathcal{D}_i)$ for every sequence $\{\mathcal{D}_i\}_{i\in\mathbb{N}}$ of sets in $\mathcal{B}_\Omega$ such that $\mathcal{D}_i \cap \mathcal{D}_i = \emptyset$ for all $i \neq j$. Then, for every probability measure representation r over Ω, we can show that the restriction of the outer measure μ_r on Ω^∞ to the Borel class $\mathcal{B}_\Omega$ is a probability measure on Ω^∞. We denote the restriction of μ_r to $\mathcal{B}_\Omega$ by μ_r just the same.

Then it is easy to see that $\mu_r\left([\sigma]^{\prec}\right) = r(\sigma)$ for every probability measure representation r over Ω and every $\sigma \in \Omega^*$.

3 Postulates of Quantum Mechanics

In this section, we recall the central postulates of quantum mechanics. For simplicity, in this paper we consider the postulates of quantum mechanics for a *finite-dimensional* quantum system, i.e., a quantum system whose state space is a finite-dimensional Hilbert space. See e.g. Nielsen and Chuang [7, Section 2] for the detail of the postulates of quantum mechanics, in particular, in the finite-dimensional case. We refer to the postulates from it. Note that these postulates are about pure states. We will consider the postulates of quantum mechanics about mixed states and their refinements later.

The first postulate of quantum mechanics is about *state space* and *state vector*.

Postulate 1 (State space and state vector)**.** *Associated to any isolated physical system is a complex vector space with inner product (i.e., Hilbert space) known as the* state space *of the system. The system is completely described by its* state vector*, which is a unit vector in the system's state space.* □

The second postulate of quantum mechanics is about the *composition* of systems.

Postulate 2 (Composition of systems)**.** *The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered* 1 *through* n*, and system number* i *is represented in the state* $|\Psi_i\rangle$*, then the joint state of the total system is* $|\Psi_1\rangle \otimes |\Psi_2\rangle \otimes \cdots \otimes |\Psi_n\rangle$. □

The third postulate of quantum mechanics is about the *time-evolution* of closed quantum systems.

Postulate 3 (Unitary time-evolution)**.** *The evolution of a* closed *quantum system is described by a* unitary transformation*. Namely, the state* $|\Psi_1\rangle$ *of the system at time* t_1 *is related to the state* $|\Psi_2\rangle$ *of the system at time* t_2 *by a unitary operator* U*, which depends only on the times* t_1 *and* t_2*, in such a way that* $|\Psi_2\rangle = U|\Psi_1\rangle$. □

The forth postulate of quantum mechanics is about *measurements* on quantum systems. This is the so-called *Born rule*, i.e, *the probability interpretation of the wave function.*

Postulate 4 (The Born rule)**.** *Quantum measurement is described by an* observable*,* M*, a Hermitian operator on the state space of the system being measured. The observable has a spectral decomposition* $M = \sum_m mE_m$*, where* E_m *is the projector onto the eigenspace of* M

with eigenvalue m. The possible outcomes of the measurement correspond to the eigenvalues, m, of the observable. If the state of the quantum system is $|\Psi\rangle$ immediately before the measurement then the probability *that result m occurs is given by $\langle\Psi|E_m|\Psi\rangle$, and the state of the system after the measurement is*

$$\frac{E_m|\Psi\rangle}{\sqrt{\langle\Psi|E_m|\Psi\rangle}}. \qquad \square$$

Thus, the Born rule, Postulate 4, uses the notion of probability. However, the operational characterization of the notion of probability is not given in the Born rule, and therefore the relation of its statement to a specific infinite sequence of outcomes of quantum measurements which are being generated by an infinitely repeated measurements is unclear. In this paper we fix this point.

We keep Postulates 1, 2, and 3 in their original forms without any modifications in this paper. We propose Postulate 5 below as a *refinement* of Postulate 4 based on the notion of *Martin-Löf P-randomness.*

4 Martin-Löf P-Randomness

In this section we introduce the notion of *Martin-Löf randomness with respect to Bernoulli measure*, which is called the Martin-Löf P-randomness in this paper. We first review the notions of *finite probability space* and *Bernoulli measure.* Both of them are from measure theory.

Definition 1 (Finite probability space)**.** *Let Ω be an alphabet. A* finite probability space on Ω *is a function $P\colon \Omega \to [0,1]$ such that (i) $P(a) \geq 0$ for every $a \in \Omega$, and (ii) $\sum_{a\in\Omega} P(a) = 1$. The set of all finite probability spaces on Ω is denoted by $\mathbb{P}(\Omega)$.* □

Let $P \in \mathbb{P}(\Omega)$. For each $\sigma \in \Omega^*$, we use $P(\sigma)$ to denote $P(\sigma_1)P(\sigma_2)\dots P(\sigma_n)$ where $\sigma = \sigma_1\sigma_2\dots\sigma_n$ with $\sigma_i \in \Omega$. For each subset S of Ω^*, we use $P(S)$ to denote $\sum_{\sigma\in S} P(\sigma)$.

Consider a function $r\colon \Omega^* \to [0,1]$ such that $r(\sigma) = P(\sigma)$ for every $\sigma \in \Omega^*$. It is then easy to see that the function r is a probability measure representation over Ω. The probability measure μ_r induced by r is called a *Bernoulli measure on Ω^∞*, denoted λ_P. The Bernoulli measure λ_P on Ω^∞ satisfies that $\lambda_P\left([\sigma]^{\prec}\right) = P(\sigma)$ for every $\sigma \in \Omega^*$.

Martin-Löf P-randomness is defined as follows. This notion was, in essence, introduced by Martin-Löf [6], as well as the notion of Martin-Löf randomness.

Definition 2 (Martin-Löf P-randomness)**.** *Let $P \in \mathbb{P}(\Omega)$. A subset $\mathcal{C}$ of $\mathbb{N}^+ \times \Omega^*$ is called a* Martin-Löf P-test *if $\mathcal{C}$ is a recursively enumerable set such that for every $n \in \mathbb{N}^+$ it holds that $\lambda_P\left([\mathcal{C}_n]^{\prec}\right) < 2^{-n}$ where $\mathcal{C}_n := \{\, \sigma \mid (n,\sigma) \in \mathcal{C} \,\}$.*

For any $\alpha \in \Omega^\infty$, we say that α is Martin-Löf P-random *if for every Martin-Löf P-test $\mathcal{C}$ there exists $n \in \mathbb{N}^+$ such that $\alpha \notin [\mathcal{C}_n]^{\prec}$.* □

In the case where $\Omega = \{0,1\}$ and P satisfies that $P(0) = P(1) = 1/2$, Bernoulli measure λ_P results in Lebesgue measure on $\{0,1\}^\infty$. In this case, the Martin-Löf P-randomness results in the Martin-Löf randomness.

5 A Refinement of the Born Rule

Let Ω be an alphabet consisting of reals. Suppose that Ω is the set of all possible measurement outcomes in a quantum measurement. Let us identify the form of the postulate of quantum measurements as it ought to be, from a general point of view. Consider an infinite sequence α of the outcomes of quantum measurements such as $\alpha = a_1a_2a_3\dots\dots$ with $a_i \in \Omega$, which is being generated as measurements progressed. All that the experimenter of quantum measurements can obtain through the measurements about quantum system is such a specific infinite sequence of outcomes in Ω of the measurements which are being generated by infinitely repeated measurements. Thus, *the object about which the postulate of quantum measurements makes a statement should be the properties of a specific infinite sequence $\alpha \in \Omega^\infty$ of outcomes of the measurements.*

Suggested by this consideration, we propose to replace the Born rule, Postulate 4, by the following postulate:

Postulate 5 (Refinement of the Born rule for pure states)**.** *Quantum measurement is described by an* observable*, M, a Hermitian operator on the state space of the system being measured. The observable has a spectral decomposition*

$$M = \sum_{m\in\Omega} mE_m$$

, where E_m is the projector onto the eigenspace of M with eigenvalue m. The set of possible outcomes of the measurement is the spectrum Ω of M. Suppose that the measurements are repeatedly performed over identical quantum systems whose states are all $|\Psi\rangle$, and the infinite sequence $\alpha \in \Omega^\infty$ of measurement outcomes is being generated. Then α is Martin-Löf P-random, where P is a finite probability space on Ω such that $P(m) = \langle\Psi|E_m|\Psi\rangle$ for every $m \in \Omega$. For each of the measurements, the state of the system immediately after the measurement is

$$\frac{E_m|\Psi\rangle}{\sqrt{\langle\Psi|E_m|\Psi\rangle}}, \tag{1}$$

where m is the corresponding measurement outcome. □

Based on the results of the works [10, 11, 12], we can see that Postulate 5 is certainly a refinement of the Born rule, Postulate 4, from the point of view of our intuitive understanding of the notion of probability.

First, according to Postulate 5 we can show that the *law of large numbers*, i.e., the *frequency interpretation*, holds for the infinite sequence $\alpha \in \Omega^\infty$ in Postulate 5. This is confirmed by the following theorem. See Tadaki [12, Section 5] for the proof.

Theorem 3 (The law of large numbers)**.** *Let Ω be an alphabet, and let $P \in \mathbb{P}(\Omega)$. For every $\alpha \in \Omega^\infty$, if α is Martin-Löf P-random then for every $a \in \Omega$ it holds that $\lim_{n\to\infty} N_a(\alpha\restriction_n)/n = P(a)$, where $N_a(\sigma)$ denotes the number of the occurrences of a in σ for every $a \in \Omega$ and $\sigma \in \Omega^*$.* □

Secondly, according to Postulate 5 we can show that an elementary event with probability one always occurs in the infinite sequence $\alpha \in \Omega^\infty$ in Postulate 5. This fact that *an elementary event with probability one occurs certainly in quantum mechanics* is derived as follows.

Recall that there is a postulate about quantum measurements with no reference to the notion of probability. This is given in Dirac [3, Section 10], and describes a spacial case of quantum measurements which are performed upon a quantum system in an *eigenstate* of an observable, i.e., a state represented by an eigenvector of an observable.

Postulate 6 (Dirac [3])**.** *If the dynamical system is in an eigenstate of a real dynamical variable ξ, belonging to the eigenvalue ξ', then a measurement of ξ will certainly gives as result the number ξ'.* □

Here, the "dynamical system" means quantum system, and the "real dynamical variable" means observable.

Based on Postulates 1, 4, and 6 above, we can show that an elementary event "with probability one" occurs certainly in quantum mechanics. To see this, let us consider a quantum system with finite-dimensional state space, and a measurement described by an observable M performed upon the system. Suppose that the probability of getting result m_0 is one in the measurement performed upon the system in a state represented by a state vector $|\Psi\rangle$. Let $M = \sum_m mE_m$ be a spectral decomposition of the observable M, where E_m is the projector onto the eigenspace of M with eigenvalue m. Then, it follows from Postulate 4 that $\langle\Psi|E_{m_0}|\Psi\rangle = 1$. This implies that $|\Psi\rangle$ is an eigenvector of M belonging to the eigenvalue m_0, since $|\Psi\rangle$ is a unit vector. Thus, we have that immediately before the measurement, the quantum system is in an eigenstate of the observable M, belonging to the eigenvalue m_0. It follows from Postulate 6 that the measurement of M will *certainly* gives as result the number m_0. Hence, it turns out that *an elementary event with probability one occurs certainly in quantum mechanics.*

Theorem 4 below confirms that an event with probability one always occurs in the infinite sequence $\alpha \in \Omega^\infty$ in Postulate 5. This result strengthens the validity of Postulate 5. Theorem 4 was, in essence, pointed out by Martin-Löf [6]. See Tadaki [12, Section 5] for the proof.

Theorem 4. *Let $P \in \mathbb{P}(\Omega)$, and let $a \in \Omega$. Suppose that α is Martin-Löf P-random and $P(a) = 1$. Then α consists only of a, i.e., $\alpha = aaaaaa\dots\dots$.* □

Thirdly, we can verify the *self-consistency* of Postulate 5 on some level, based on the arguments given in Tadaki [12, Sections 5.3 and 5.4]. This suggests that Postulate 5 is not too strong.

Postulate 5 is based on the notion of Martin-Löf P-randomness. In general, we can use this notion to present *an operational characterization of the notion of probability*, and we can reformulate probability theory based on the notion of Martin-Löf P-randomness. For example, we can represent the notion of *conditional probability* and the notion of *the independence of events/random variables* in terms of Martin-Löf P-randomness. Thus, Martin-Löf P-randomness is thought to reflect all the properties of the notion of probability from our intuitive understanding of the notion of probability. Hence, *Postulate 5, which uses the notion of Martin-Löf P-randomness, is thought to be a rigorous reformulation of Postulate 4.* The detail of the operational characterization was reported in [10, 11, 12].

We will later show that Postulate 5 can be derived from a postulate, called the *principle of typicality*, together with Postulates 1, 2, and 3.

6 Mixed States

Postulate 4 above is the Born rule for pure states. Recall that the Born rule for mixed states is given as follows.

Postulate 7 (The Born rule for mixed states)**.** *Quantum measurement is described by an* observable*, M, a Hermitian operator on the state space of the system being measured. The observable has a spectral decomposition $M = \sum_m mE_m$, where E_m is the projector onto the eigenspace of M with eigenvalue m. The possible outcomes of the measurement correspond to the eigenvalues, m, of the observable. If the state of the quantum system is represented by a density matrix ρ immediately before the measurement then the* probability *that result m occurs is given by $\operatorname{tr}(E_m\rho)$, and the state of the system after the measurement is $E_m\rho E_m/\operatorname{tr}(E_m\rho)$.* □

We propose a refinement of Postulate 7 by algorithmic randomness in what follows. First, note that according to Postulate 5, the result of the quantum measurements forms a Martin-Löf P-random infinite sequence of pure states, each of which is of the form (1). On the other hand, in the conventional quantum mechanics this measurement result is described as a mixed state. Suggested by these facts, we propose a *mathematical definition of the notion of a mixed state* in terms of Martin-Löf P-randomness, as follows.

Definition 5 (Mixed state and its density matrix)**.** *Let $\mathcal{S}$ be a quantum system with state space $\mathcal{H}$ of finite dimension. Let Ω be a non-empty finite set of state vectors in $\mathcal{H}$, and let $\alpha \in \Omega^\infty$. We say that α is a* mixed state *of $\mathcal{S}$ if there exists a finite probability space P on Ω such that α is a Martin-Löf P-random. The* density matrix *ρ of the mixed state α is defined by*

$$\rho := \sum_{|\Psi\rangle\in\Omega} P(|\Psi\rangle)|\Psi\rangle\langle\Psi|,$$

where P is a finite probability space on Ω for which α is Martin-Löf P-random. □

Note that the definition of density matrix given in Definition 5 is the same as in the conventional quantum mechanics. Using this rigorous definition of mixed state, we propose to replace the Born rule for mixed states, Postulate 7, by the following rule of an operational form based on Martin-Löf P-randomness.

Postulate 8 (Refinement of the Born rule for mixed states)**.** *Quantum measurement is described by an* observable*, M, a Hermitian operator on the state space of the system being measured. The observable has a spectral decomposition $M=\sum_{m\in\Omega} mE_m$, where E_m is the projector onto the eigenspace of M with eigenvalue m. The set of possible outcomes of the measurement is the spectrum Ω of M. Suppose that the measurements are repeatedly performed over a mixed state with a density matrix ρ. Then the infinite sequence of outcomes generated by the measurements is a Martin-Löf P-random infinite sequence over Ω, where P is a finite probability space on Ω such that $P(m)=\operatorname{tr}(E_m\rho)$ for every $m\in\Omega$. Moreover, the resulting sequence of pure states with outcome m is a mixed state with the density matrix $E_m\rho E_m/\operatorname{tr}(E_m\rho)$.* □

7 The Many-Worlds Interpretation of Quantum Mechanics

In what follows, we consider the validity of our new rules, Postulates 5 and 8, from the point of view of the *many-worlds interpretation of quantum mechanics* (*MWI*, for short) introduced by Everett [5] in 1957. More specifically, we derive Postulates 5 and 8 based on a *refinement* of the arguments in MWI, called the *principle of typicality.*

To begin with, we review the framework of MWI. MWI is more than just an interpretation of quantum mechanics. It aims to derive Postulate 4 from the remaining postulates, Postulates 1, 2, and 3. In this sense, Everett [5] proposed MWI as a "metatheory" of quantum mechanics. The point is that in MWI the measurement process is fully treated as the interaction between a system and an apparatus, based only on Postulates 1, 2, and 3. Then MWI tries to derive Postulate 4 in such a setting.

Let us investigate the setting of MWI in terms of our terminology. According to Postulates 1, 2, and 3, we consider the following unitary operator U which describes the interaction between a system and an apparatus as measurement process:

$$U|m\rangle\otimes|\Phi^{\text{init}}\rangle=|m\rangle\otimes|\Phi[m]\rangle. \tag{2}$$

Here, $|m\rangle$ is an eigenstate of an observable of the system where $\{|m\rangle\}$ forms an orthonormal basis of the state space of the system.[1] The vector $|\Phi^{\text{init}}\rangle$ is the initial state of the apparatus, and $|\Phi[m]\rangle$ is the final state of the apparatus with $\langle\Phi[m]|\Phi[m']\rangle=\delta_{m,m'}$. By this interaction, a correlation (i.e., entanglement) is generated between the system and the apparatus. The state $|\Phi[m]\rangle$ indicates that *the apparatus records the value m of the observable of the system.*

Actually, we consider an infinite repetition of measurements of an identical observable over identical systems prepared in an identical state, each of which is described by the unitary time-evolution (2). As measurements progressed, correlations between the systems and the apparatus are being generated in sequence in the superposition of the total system consisting of the systems and the apparatus. The detail is described as follows.

For simplicity, we here consider the measurements over qubit systems. Let $|0\rangle$ and $|1\rangle$ be an orthonormal basis of the state space of a qubit system. We prepare countably infinite qubit systems in an identical state $|\Psi\rangle:=C(0)|0\rangle+C(1)|1\rangle$ with $C(k)\in\mathbb{C}$ and perform measurements of the observable $|1\rangle\langle 1|$ over these qubit systems one by one by interacting an apparatus with these qubit systems one by one. Let $\mathcal{H}_n$ be the state space of the total system consisting of the first n qubit systems and the apparatus. The successive interaction between the qubit systems and the apparatus as measurement process proceeds in the following manner.

The initial state of the total system, which consists of the first qubit system and the apparatus, is $|\Psi\rangle\otimes|\Phi^{\text{init}}\rangle\in\mathcal{H}_1$. Immediately after the measurement of the first qubit system, the total system results in the state $\sum_{a_1=0,1}C(a_1)|a_1\rangle\otimes|\Phi[a_1]\rangle\in\mathcal{H}_1$ by the interaction (2) as measurement process. In general, immediately before the measurement of the nth qubit system, the state of the total system, which consists of the first n qubit systems and the apparatus, is

$$\sum_{a_1,\dots,a_{n-1}=0,1} C(a_1)\cdots C(a_{n-1})\,|a_1\rangle\otimes\cdots\otimes|a_{n-1}\rangle\otimes|\Psi\rangle \otimes|\Phi[a_1\dots a_{n-1}]\rangle\otimes|\Phi^{\text{init}}\rangle$$

in $\mathcal{H}_n$, where $|\Phi[a_1\dots a_{n-1}]\rangle$ denotes $|\Phi[a_1]\rangle\otimes\cdots\otimes|\Phi[a_{n-1}]\rangle$. Immediately after the measurement of the nth qubit system, the total system results in the state

$$\sum_{a_1,\dots,a_n=0,1} C(a_1)\cdots C(a_n)\,|a_1\rangle\otimes\cdots\otimes|a_n\rangle \otimes|\Phi[a_1\dots a_n]\rangle \tag{3}$$

by the interaction (2) between the nth qubit system in the state $|\Psi\rangle$ and the apparatus in the state $|\Phi^{\text{init}}\rangle$ as measurement process. The state $|\Phi[a_1\dots a_n]\rangle$ indicates that *the apparatus records the values $a_1\dots a_n$ of the observables $|1\rangle\langle 1|$ of the first n qubit systems.*

In the above description, on letting $n\to\infty$, a *world* is defined as the infinite sequence of records of the values of the observable in the apparatus. Thus, the finite records $a_1\dots a_n$ in each state $|\Phi[a_1\dots a_n]\rangle$ in the superposition (3) of the total system is a prefix of a world. Each world is an infinite binary sequence in this case of the total system consisting of the qubit systems and the apparatus.

[1] For simplicity, we here consider the case where the measured observable has no degeneracy. An extension of the general case with degeneracy is obvious.

Then, for aiming at deriving Postulate 4, MWI assigns "weight" to each of worlds. Namely, it introduces measure on the set of all worlds in the following manner. First, MWI introduces a probability measure representation on the set of prefixes of worlds, i.e., the set $\{0,1\}^*$ in this case. This probability measure representation is given by a function $r\colon \{0,1\}^* \to [0,1]$ with $r(a_1 \dots a_n) = |C(a_1)\cdots C(a_n)|^2$, which is the square of the norm of each state $C(a_1)\cdots C(a_n)\,|a_1\rangle \otimes \cdots \otimes |a_n\rangle \otimes |\Phi[a_1 \dots a_n]\rangle$ in the superposition (3). We can easily check that r is certainly a probability measure representation. The measure induced by the probability measure representation r is just the Bernoulli measure λ_P on $\{0,1\}^\infty$, where P is a finite probability space on $\{0,1\}$ such that $P(a) = |C(a)|^2$ for every $a \in \{0,1\}$.

Let $R \subset \{0,1\}^\infty$ be a "typical" property with respect to the Bernoulli measure λ_P. Namely, let R be a Borel subset of $\{0,1\}^\infty$, i.e., $R \in \mathcal{B}_{\{0,1\}}$, such that $\lambda_P(R) = 1$. For example, we can consider as R the set of worlds for which the frequency interpretation, i.e., the law of large numbers, holds. By definition, the property R holds in "almost all" worlds. Based on this arguments, MWI insists that Postulate 4 has been derived from Postulates 1, 2, and 3. In this argument by Everett [5], however, what is typical is just a set R of worlds and not an individual world. The problem here is *whether our world is in R, or not.* The argument by Everett is unclear in this regard. Moreover, as we already pointed out, there is no operational characterization of the notion of probability in Postulate 4 while it makes a statement about the probability of measurement outcomes. Therefore, what MWI has to show for deriving Postulate 4 is unclear. By contrast, the replacement of Postulate 4 by Postulate 5 makes this clear since there is no ambiguity in Postulate 5 from the operational point of view.

8 The Principle of Typicality

As we saw in the preceding section, for deriving the Born rule, Postulate 4, MWI seems to assume that our world is "typical" or "random' among many coexisting worlds. However, the proposal of MWI by Everett was nearly a decade earlier than the advent of algorithmic randomness. Actually, Everett [5] proposed MWI in 1957 while the notion of Martin-Löf randomness was introduced by Martin-Löf [6] in 1966. Thus, the assumption of "typicality" by Everett in MWI was not rigorous from a mathematical point of view.

The notion of "typicality" or "randomness" is just the research object of algorithmic randomness. Based on the notion of Martin-Löf P-randomness, we introduce a postulate, called the *principle of typicality* as follows. The principle of typicality is a *refinement* of the assumption of "typicality" by Everett [5].

Postulate 9 (The principle of typicality)**.** *Our world is typical. Namely, our world is Martin-Löf random with respect to the measure on the set of all worlds, induced by the probability measure representation defined as the square of the norm of each state in the superposition of the total system.* □

In the case of the total system consisting of the qubit systems and the apparatus which we considered in the preceding section, the probability measure representation and the measure referred to in Postulate 9 are r and λ_P, respectively. Hence, Postulate 9 is precisely Postulate 5 in this case. It is easy to see that in the case where we treat only pure states, Postulate 9 is precisely Postulate 5 in general. Thus, Postulate 5 is derived from Postulate 9 together with Postulates 1, 2, and 3.

We can derive Postulate 8 from Postulate 9 together with Postulates 1, 2, and 3 in several scenarios of the setting of measurements. We can do this by considering more complicated interaction between systems and apparatus than one used for deriving Postulate 5 in the above. Recall that mixed state on which measurements are performed is an infinite sequence of pure states, as defined in Definition 5. Hence, we have to perform measurements on the mixed state while generating it. We have investigated several scenarios which implement this setting. In all the scenarios which we considered so far, Postulate 8 can be derived from Postulate 9 together with Postulates 1, 2, and 3.

9 Application to Quantum Cryptography

In this section, we make an application of our framework to the BB84 quantum key distribution protocol [1] in order to demonstrate how properly our framework works in a practical problem *based on the principle of typicality.* For the simplicity of the analysis, we consider the following slight modification of the original BB84 protocol [1]. Let $|\Psi_{00}\rangle := |0\rangle$, $|\Psi_{10}\rangle := |1\rangle$, $|\Psi_{01}\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$, and $|\Psi_{11}\rangle := (|0\rangle - |1\rangle)/\sqrt{2}$.

Protocol 6 (The BB84 QKD protocol with slight modifications)**.** Initially, set flag := 0. Repeat the following procedure forever.

Step 1: Alice tosses two fair coins A and B to get outcomes a and b in $\{0,1\}$, respectively.

Step 2: Alice prepares $|\Psi_{ab}\rangle$ and sends it to Bob.

Step 3: Bob tosses a fair coin C to get outcome $c \in \{0,1\}$.

Step 4: Bob performs the measurement of the observable $|\Psi_{1c}\rangle\langle\Psi_{1c}|$ over the state $|\Psi_{ab}\rangle$ to obtain outcome $m \in \{0,1\}$.

Step 5: Bob tosses a biased coin D to get outcome $d \in \{0,1\}$, where $\Pr\{D = 1\} = p$.

Step 6: If flag = 1, Alice and Bob discard all the bits obtained so far.

Step 7: Alice and Bob announce b and c, respectively.

Step 8: If $b \neq c$, Alice and Bob discard a and m and then go to Step 1.

Step 9: If $d = 0$, Alice and Bob keep a and m, respectively, *as a shared random bit*, and then go to Step 1.

Step 10: Alice and Bob announce a and m.

Step 11: If $a \neq m$, Alice and Bob set flag := 1.

Step 12: Alice and Bob discard a and m. □

In what follows, we investigate Protocol 6 based on Postulate 9, without Postulate 4 and without even Postulate 5, from the point of view of our refinement of MWI. To complete this, we have to implement everything in Steps 1–5 of Protocol 6 by unitary time-evolution.

First, we consider the case where there is no eavesdropping. We describe the interaction between a system and an apparatus as measurement process, as described in (2). The interaction is divided into the following five unitary time-evolutions.

To realize the coin tossing in Step 1 of Protocol 6 we make use of measurement over two qubits system. The measurement is described by the unitary time-evolution $U_1|ab\rangle\otimes|\Phi_1^{\text{init}}\rangle = |ab\rangle\otimes|\Phi_1[ab]\rangle$ $(a, b \in \{0,1\})$, where $|ab\rangle := |a\rangle \otimes |b\rangle$ is a state of the two qubits system, and $|\Phi_1^{\text{init}}\rangle$ and $|\Phi_1[ab]\rangle$ are states of an apparatus. Prior to the measurement, the two qubits system is prepared in the state $|\Psi_{01}\rangle \otimes |\Psi_{01}\rangle$. The preparation of the state $|\Psi_{ab}\rangle$ by Alice in Step 2 is realized by the unitary time-evolution $U_2|\Phi_1[ab]\rangle\otimes|\Psi_{00}\rangle = |\Phi_1[ab]\rangle \otimes |\Psi_{ab}\rangle$ $(a, b \in \{0,1\})$. Then, similarly to Step 1, the coin tossing in Step 3 is described by the unitary time-evolution $U_3|c\rangle\otimes|\Phi_3^{\text{init}}\rangle = |c\rangle\otimes|\Phi_3[c]\rangle$ $(c \in \{0,1\})$.

The switching of the two types of measurements in Step 4, depending on the outcome c, is realized by the unitary time-evolution $U_4|\Phi_3[c]\rangle\otimes|\Theta\rangle = |\Phi_3[c]\rangle\otimes V_c|\Theta\rangle$. Here, the unitary time-evolution $V_c|\Psi_{ac}\rangle \otimes |\Phi_4^{\text{init}}\rangle = |\Psi_{ac}\rangle \otimes |\Phi_4[a]\rangle$ $(a, c \in \{0,1\})$ is applied to the composite system consisting of the qubit sent from Alice and an apparatus, and describes the alternate measurement process of the qubit sent from Alice, depending on the outcome c. Note that the unitarity of U_4 is confirmed by the following theorem.

Theorem 7. *Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be finite-dimensional Hilbert spaces. Let $\{|1\rangle, \dots, |N\rangle\}$ be an orthonormal basis of $\mathcal{H}_1$, and let $U_1, \dots, U_N$ be arbitrary N unitary operators on $\mathcal{H}_2$. Then $U := |1\rangle\langle 1| \otimes U_1 + \dots + |N\rangle\langle N| \otimes U_N$ is a unitary operator on $\mathcal{H}_1 \otimes \mathcal{H}_2$, and $U(|k\rangle \otimes |\Psi\rangle) = |k\rangle\otimes(U_k|\Psi\rangle)$ for every $k = 1, \dots, N$ and $|\Psi\rangle \in \mathcal{H}_2$.* □

Finally, the biased coin tossing in Step 5 is described by the unitary time-evolution $U_5|d\rangle \otimes |\Phi_5^{\text{init}}\rangle = |d\rangle \otimes |\Phi_5[d]\rangle$ $(d \in \{0,1\})$ similarly to Step 3, while a qubit system is prepared in the state $\sqrt{1-p}|0\rangle + \sqrt{p}|1\rangle$ instead of $|\Psi_{01}\rangle$ prior to the measurement.

The sequential application of $U_1, \dots, U_5$ to the composite system consisting of four qubits system and apparatus results in the following single unitary time-evolution U: (i) if $b = c$ then

$$U|abcd\rangle \otimes |\Psi_{00}\rangle \otimes |\Phi^{\text{init}}\rangle = |abcd\rangle \otimes |\Psi_{ab}\rangle \otimes |\Phi[abcad]\rangle,$$

and (ii) if $b \neq b$ then

$$U|abcd\rangle \otimes |\Psi_{00}\rangle \otimes |\Phi^{\text{init}}\rangle = \frac{1}{\sqrt{2}}|abcd\rangle \otimes |\Psi_{0c}\rangle \otimes |\Phi[abc0d]\rangle + \frac{(-1)^a}{\sqrt{2}}|abcd\rangle \otimes |\Psi_{1c}\rangle \otimes |\Phi[abc1d]\rangle.$$

Here, $|abcd\rangle$ denotes the four qubits state $|a\rangle\otimes|b\rangle\otimes|c\rangle\otimes|d\rangle$, $|\Phi^{\text{init}}\rangle$ denotes $|\Phi_1^{\text{init}}\rangle\otimes|\Phi_3^{\text{init}}\rangle\otimes|\Phi_4^{\text{init}}\rangle\otimes|\Phi_5^{\text{init}}\rangle$, and $|\Phi[abcmd]\rangle$ denotes $|\Phi_1[ab]\rangle\otimes|\Phi_3[c]\rangle\otimes|\Phi_4[m]\rangle\otimes|\Phi_5[d]\rangle$. Totally, prior to the application of U, the four qubits system is prepared in the state

$$\sum_{abcd \in \{0,1\}^4} \frac{1}{\sqrt{8}} \mathcal{A}_d |abcd\rangle,$$

where $\mathcal{A}_0 = \sqrt{1-p}$ and $\mathcal{A}_1 = \sqrt{p}$.

Let Ω be the alphabet $\{0,1\}^5$, which is the set of all possible records of the apparatus in a repeated once of the procedure in Protocol 6. It follows from Postulate 9, the principle of typicality, that our world, i.e., the infinite sequence $\alpha \in \Omega^\infty$ of records in the apparatus which is being generated by the infinite repetition of the procedure in Protocol 6, is Martin-Löf P-random, where P is a finite probability space on Ω such that (i) in the case of $b = c$, $P(abcmd) = \mathcal{A}_d^2/8$ if $a = m$ and $P(abcmd) = 0$ otherwise, and (ii) in the case of $b \neq c$, $P(abcmd) = \mathcal{A}_d^2/16$.

Let β be an infinite sequence over Ω obtained from α by eliminating all elements of the form $abcmd$ with $b \neq c$ occurring in α. Using Theorem 18 of Tadaki [12] and Theorem 4 in this paper we can show the following: First, β consists only of elements of the form $abbad$. This shows that Alice and Bob certainly share an identical bit every time of the case of $b = c$. Let γ be an infinite binary sequence obtained from β by replacing each element $abbad$ in β by a. We then see that γ is *Martin-Löf random*. This means that Alice and Bob certainly share a "random" infinite binary sequence.

Next, we consider the case where there is an eavesdropping by Eve. We assume that Eve performs the following eavesdropping between Step 2 and Step 3 of Protocol 6.

Step E1: Eve tosses a fair coin E to get outcome $e \in \{0,1\}$.

Step E2: Eve performs the measurement of the observable $|\Psi_{1e}\rangle\langle\Psi_{1e}|$ over the state $|\Psi_{ab}\rangle$ sent from Alice to Bob, and obtains outcome $f \in \{0,1\}$.

Steps E1 and E2 are the same as Steps 3 and 4 of Protocol 6. Thus, it is easy to see that Eve performs the following unitary time-evolution U_{Eve} on the composite system consisting of a two qubits system and an apparatus: $U_{\mathrm{Eve}}|e\rangle \otimes |\Phi_{E1}^{\mathrm{init}}\rangle \otimes |\Psi_{ab}\rangle \otimes |\Phi_{E2}^{\mathrm{init}}\rangle = |e\rangle \otimes |\Phi_{E1}[e]\rangle \otimes \widetilde{V_e}(|\Psi_{ab}\rangle \otimes |\Phi_{E2}^{\mathrm{init}}\rangle)$, where the unitary operator $\widetilde{V_e}$ satisfies that $\widetilde{V_e}|\Psi_{ae}\rangle \otimes |\Phi_{E2}^{\mathrm{init}}\rangle = |\Psi_{ae}\rangle \otimes |\Phi_{E2}[a]\rangle$. The vector $|e\rangle$ is a state of a qubit system which implements the tossing of a fair coin in Step E1, and $|\Phi_{E1}^{\mathrm{init}}\rangle$ and $|\Phi_{E1}[e]\rangle$ are states of an apparatus measuring the qubit system. Prior to the measurement, the qubit system is prepared in the state $|\Psi_{01}\rangle$. The vectors $|\Phi_{E2}^{\mathrm{init}}\rangle$ and $|\Phi_{E2}[a]\rangle$ are states of an apparatus measuring the qubit system with state $|\Phi_{ab}\rangle$ sent from Alice to Bob in Step E2.

The sequential application of $U_1, U_2, U_{\mathrm{Eve}}, U_3, U_4, U_5$ to the composite system consisting of five qubits system and apparatus results in a single unitary time-evolution $\widetilde{U}$ which satisfies that: (i) If $b = c = e$ then

$$\begin{aligned}&\widetilde{U}|abecd\rangle \otimes |\Psi_{00}\rangle \otimes |\Phi^{\mathrm{init}}\rangle \\ &\quad = |abecd\rangle \otimes |\Psi_{ab}\rangle \otimes |\Phi[abeacad]\rangle;\end{aligned}$$

(ii) If $b = c \neq e$ then

$$\begin{aligned}&\widetilde{U}|abecd\rangle \otimes |\Psi_{00}\rangle \otimes |\Phi^{\mathrm{init}}\rangle \\ &= \frac{1}{2}|abecd\rangle \otimes |\Psi_{0c}\rangle \otimes |\Phi[abe0c0d]\rangle \\ &+ \frac{1}{2}|abecd\rangle \otimes |\Psi_{1c}\rangle \otimes |\Phi[abe0c1d]\rangle \\ &+ \frac{(-1)^a}{2}|abecd\rangle \otimes |\Psi_{0c}\rangle \otimes |\Phi[abe1c0d]\rangle \\ &- \frac{(-1)^a}{2}|abecd\rangle \otimes |\Psi_{1c}\rangle \otimes |\Phi[abe1c1d]\rangle.\end{aligned}$$

Here, $|abecd\rangle$ denotes the five qubits state $|a\rangle \otimes |b\rangle \otimes |e\rangle \otimes |c\rangle \otimes |d\rangle$, $|\Phi^{\mathrm{init}}\rangle$ denotes $|\Phi_1^{\mathrm{init}}\rangle \otimes |\Phi_{E1}^{\mathrm{init}}\rangle \otimes |\Phi_{E2}^{\mathrm{init}}\rangle \otimes |\Phi_3^{\mathrm{init}}\rangle \otimes |\Phi_4^{\mathrm{init}}\rangle \otimes |\Phi_5^{\mathrm{init}}\rangle$, and $|\Phi[abefcmd]\rangle$ denotes $|\Phi_1[ab]\rangle \otimes |\Phi_{E1}[e]\rangle \otimes |\Phi_{E2}[f]\rangle \otimes |\Phi_3[c]\rangle \otimes |\Phi_4[m]\rangle \otimes |\Phi_5[d]\rangle$. Totally, prior to the application of $\widetilde{U}$, the five qubits system is prepared in the state

$$\sum_{abecd \in \{0,1\}^5} \frac{1}{4}\mathcal{A}_d|abecd\rangle,$$

where $\mathcal{A}$'s are the same as before.

Let Ω_E be the alphabet $\{0,1\}^7$, which is the set of all possible records of the apparatus in a repeated once of the procedure in Protocol 6 with the eavesdropping by Eve. It follows from Postulate 9 that our world, i.e., the infinite sequence $\alpha_E \in \Omega_E^\infty$ of records in the apparatus which is being generated by the infinite repetition of the procedure in Protocol 6 with the eavesdropping by Eve, is Martin-Löf P_E-random, where P_E is a finite probability space on Ω_E such that (i) in the case of $b = c = e$, $P_E(abefcmd) = \mathcal{A}_d^2/16$ if $f = a$ & $m = a$ and $P_E(abefcmd) = 0$ otherwise, and (ii) in the case of $b = c \neq e$, $P_E(abefcmd) = \mathcal{A}_d^2/64$.

Let β_E be an infinite sequence over Ω_E obtained from α_E by eliminating all elements of the form $abefcmd$ with $b \neq c$ or $d = 0$ occurring in α_E. As in the case of no eavesdropping, we can show the following: β_E consists only of elements of the form $abefbm1$. Let γ_E be an infinite binary sequence obtained from β_E by replacing each element $abefbm1$ in β_E by 0 if $a = m$ and by 1 otherwise. Then the infinite binary sequence γ_E is Martin-Löf random. This *means* the following: If every time of the case of $b = c$ and $d = 1$, Alice and Bob check whether $a \neq m$ holds by announcing a and m, they can find the eavesdropping by Eve with "probability" 1/2.

References

[1] C. H. Bennet and G. Brassard, Quantum cryptography: Public key distribution and coin tossing. *Proc.* IEEE International Conference on Computers, Systems and Signal Processing, pp.175–179, December 1984, Bangalore, India.

[2] B. S. DeWitt and N. Graham (eds.), *The Many-Worlds Interpretation of Quantum Mechanics.* Princeton University Press, Princeton, 1973.

[3] P. A. M. Dirac, *The Principles of Quantum Mechanics*, 4th ed. Oxford University Press, London, 1958.

[4] R. G. Downey and D. R. Hirschfeldt, *Algorithmic Randomness and Complexity.* Springer-Verlag, New York, 2010.

[5] H. Everett, III, ""Relative State" formulation of quantum mechanics," *Rev. Mod. Phys.*, vol. 29, no. 3, pp. 454–462, 1957.

[6] P. Martin-Löf, "The definition of random sequences," *Information and Control*, vol. 9, pp. 602–619, 1966.

[7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.

[8] A. Nies, *Computability and Randomness.* Oxford University Press, Inc., New York, 2009.

[9] K. Tadaki, Reformulating quantum mechanics by algorithmic randomness. Presentation at Ninth International Conference on Computability, Complexity and Randomness (CCR 2014), June 9-13, 2014, Institute for Mathematical Sciences, National University of Singapore, Singapore.

[10] K. Tadaki, An operational characterization of the notion of probability by algorithmic randomness. *Proc.* SITA2014, 5.4.1, pp. 389–394, December 9-12, 2014, Unazuki, Toyama, Japan.

[11] K. Tadaki, An operational characterization of the notion of probability by algorithmic randomness and its application to cryptography. *Proc.* SCIS2015, 2D4-3, January 20-23, 2015, Kokura, Japan.

[12] K. Tadaki, "An operational characterization of the notion of probability by algorithmic randomness and its applications," arXiv:1611.06201v1, November 2016.