数理解析研究所講究録 1426 巻 2005 年 212-218

Chaitin's halting probability Ω and quantum measurements in an infinite dimensional quantum system

中央大学 21 世紀 COE プログラム　只木孝太郎 (Kohtaro Tadaki)*
21st Century Center Of Excellence Program, Chuo University

Abstract. This paper proposes an extension of Chaitin's halting probability Ω to measurement operator in an infinite dimensional quantum system. Chaitin's Ω is defined as the probability that the universal self-delimiting Turing machine U halts, and plays a central role in the development of algorithmic information theory. In the theory, there are two equivalent ways to define the program-size complexity $H(s)$ of a given finite binary string s. In the standard way, $H(s)$ is defined as the length of the shortest input string for U to output s. In the other way, the so-called universal probability m is introduced first, and then $H(s)$ is defined as $-\log_2 m(s)$ without reference to the concept of program-size.

Mathematically, the statistics of outcomes in a quantum measurement are described by a positive operator-valued measure (POVM) in the most general setting. Based on the theory of computability structures on a Banach space developed by Pour-El and Richards, we extend the universal probability to an analogue of POVM in an infinite dimensional quantum system, called universal semi-POVM. We also give another characterization of Chaitin's Ω numbers by universal probabilities. Then, based on this characterization, we propose to define an extension of Ω as a sum of the POVM elements of a universal semi-POVM. The validity of this definition is discussed.

1 Introduction

Algorithmic information theory is a framework to apply information-theoretic and probabilistic ideas to recursive function theory. One of the primary concepts of algorithmic information theory is the *program-size complexity* (or *Kolmogorov complexity*) $H(s)$ of a finite binary string s, which is defined as the length of the shortest binary input for the universal self-delimiting Turing machine to output s. By the definition, $H(s)$ can be thought of as the information content of individual finite binary string s. In fact, algorithmic information theory has precisely the formal properties of classical information theory (see [2]). The concept of program-size complexity plays a crucial role in characterizing the randomness of a finite or infinite binary string. In [2] Chaitin introduced the halting probability Ω as an example of random infinite string. His Ω is defined as the probability that the universal self-delimiting Turing machine halts, and plays a central role in the development of algorithmic information theory. The first n bits of the base-two expansion of Ω solves the halting problem for a program of size not greater than n. By this property, the base-two expansion of Ω is shown to be an instance of a random infinite binary string. In [3] Chaitin encoded this random property of Ω onto an exponential Diophantine equation in the manner that a certain property of the set of the solutions of the equation is indistinguishable from coin tosses. Moreover, based on this random property of the equation, Chaitin derived several quantitative versions of Gödel's incompleteness theorems.

In [7] we generalized Chaitin's halting probability Ω to Ω^D so that the degree of randomness of Ω^D can be controlled by a real number D with $0 < D \leq 1$. As D becomes larger, the degree of randomness of Ω^D increases. When $D = 1$, Ω^D becomes a random real number, i.e., $\Omega^1 = \Omega$. The properties of Ω^D and its relations to self-similar sets were studied in [7]. In the present paper, however, we generalize Chaitin's Ω to a different direction from [7]. The aim of the present paper is to

*E-mail: tadaki@kc.chuo-u.ac.jp

extend Chaitin's halting probability Ω to measurement operator in an infinite dimensional quantum system (i.e., a quantum system whose state space has infinite dimension).

The program-size complexity $H(s)$ is originally defined using the concept of program-size, as stated above. However, it is possible to define $H(s)$ without referring to such a concept, i.e., we first introduce a *universal probability* m, and then define $H(s)$ as $-\log_2 m(s)$. A universal probability is defined through the following two definitions. We denote by Σ^* the set of finite binary strings, by $\mathbb{N}^+$ the set of positive integers, and by $\mathbb{Q}$ the set of rational numbers.

Definition 1.1. *For any $r\colon \Sigma^* \to [0,1]$, we say that r is a lower-computable semi-measure if r satisfies the two conditions: (i) $\sum_{s\in\Sigma^*} r(s) \le 1$ and (ii) there exists a total recursive function $f\colon \mathbb{N}^+ \times \Sigma^* \to \mathbb{Q}$ such that, for each $s \in \Sigma^*$, $\lim_{n\to\infty} f(n,s) = r(s)$ and $\forall n \in \mathbb{N}^+$ $0 \le f(n,s) \le f(n+1,s)$.*

Definition 1.2. *Let m be a lower-computable semi-measure. We say that m is a universal probability if for any lower-computable semi-measure r, there exists a real number $c > 0$ such that, for all $s \in \Sigma^*$, $cr(s) \le m(s)$.*

In quantum mechanics, a *positive operator-valued measure* (POVM) is the mathematical tool which describes the statistics of outcomes in a quantum measurement in the most general setting. In this paper we extend the universal probability to an analogue of a POVM in an infinite dimensional quantum system, called a *universal semi-POVM*. Then, based on universal semi-POVM, we introduce the extension $\hat{\Omega}$ of Chaitin's Ω to measurement operator in an infinite dimensional quantum system.

In the previous work [8], we developed the theory of universal semi-POVM for finite dimensional quantum system. In this paper we try to extend the work [8] over infinite dimensional setting.

1.1 Quantum measurements

Let X be a separable complex Hilbert space. We assume that the inner product $\langle u, v\rangle$ of X is linear in the first variable u and conjugate linear in the second variable v, and it is related to the norm by $\|u\| = \langle u,u\rangle^{1/2}$. $\mathcal{B}(X)$ is the set of *bounded* operators in X. We denote the *identity operator* in X by I. For each $T \in \mathcal{B}(X)$, the *adjoint* operator of T is denoted as $T^* \in \mathcal{B}(X)$. We say $T \in \mathcal{B}(X)$ is *Hermitian* if $T = T^*$. $\mathcal{B}_h(X)$ is the set of Hermitian operators in X. We say $T \in \mathcal{B}(X)$ is *positive* if $\langle Tx, x\rangle \ge 0$ for all $x \in X$. $\mathcal{B}(X)_+$ is the set of positive operators in X. For each $S, T \in \mathcal{B}_h(X)$, we write $S \leqslant T$ if $T - S$ is positive.

With every quantum system there is associated a separable complex Hilbert space X. The states of the system are described by the nonzero elements in X. In the present paper, we consider the case where X is a Hilbert space of infinite dimension. That is, we consider *infinite dimensional quantum systems*.

Let us consider a quantum measurement performed upon a quantum system. We first define a *POVM on a σ-field* as follows.

Definition 1.3. *Let $\mathcal{F}$ be a σ-field in a set Φ. We say $M\colon \mathcal{F} \to \mathcal{B}(X)_+$ is a POVM on σ-field $\mathcal{F}$ if the following holds for M: If $\{B_j\}$ is a countable partition of Φ into pairwise disjoint subsets in $\mathcal{F}$, then $\sum_j M(B_j) = I$ where the series converges strongly.*

In the most general setting, the statistics of outcomes in a quantum measurement are described by a POVM M on a σ-field in a set Φ. The Φ is a set of outcomes possible under the quantum measurement. If the state of the quantum system is described by an $x \in X$ with $\|x\| = 1$ immediately before the measurement, then the probability distribution of the measurement outcomes is given by $\langle M(B)x, x\rangle$. (See e.g. [5] for the treatment of the mathematical foundation of quantum mechanics.)

In this paper, we relate an argument s of a universal probability $m(s)$ to an individual outcome which may occur in a quantum measurement. Thus, since $m(s)$ is defined for all finite binary strings s, we focus our thought on a POVM measurement with countably infinite measurement outcomes, such as the measurement of energy level of a harmonic oscillator. Since Φ is a countably infinite set for our purpose, we particularly define the notion of *POVM on a countably infinite set* as follows.

Definition 1.4. *Let S be a countably infinite set, and let $R\colon S \to \mathcal{B}(X)_+$. We say R is a POVM on countably infinite set S if R satisfies $\sum_{v\in S} R(v) = I$ where the series converges strongly.*

Let S be a countably infinite set, and let $\mathcal{F}$ be the set of all subsets of S. Assume that $R\colon S \to \mathcal{B}(X)_+$ is a POVM on countably infinite set S in Definition 1.4. Then, by setting

$M(B) = \sum_{v \in B} R(v)$ for every $B \in \mathcal{F}$, we can show that $M\colon \mathcal{F} \to \mathcal{B}(X)$ is a POVM on σ-field $\mathcal{F}$ in Definition 1.3. Thus Definition 1.4 is sufficient for our purpose. Each operator $R(v) \in \mathcal{B}(X)_+$ is called a *POVM element.*

In a POVM measurement with countably infinite measurement outcomes, we represent each measurement outcome by just a finite binary string in perfect register with an argument of universal probability. Thus we consider the notion of *POVM on* Σ^* which is a special case of POVM on a countably infinite set.

Definition 1.5 (POVM on Σ^*). *We say $R\colon \Sigma^* \to \mathcal{B}(X)_+$ is a POVM on Σ^* if R is a POVM on countably infinite set Σ^*.*

In a quantum measurement described by a POVM on Σ^*, an experimenter gets a finite binary string as a measurement outcome.

Any universal probability m satisfies $\sum_{s \in \Sigma^*} m(s) < 1$. This relation is incompatible with the relation $\sum_{s \in \Sigma^*} R(s) = I$ satisfied by a POVM R on Σ^*. Hence we further introduce the notion of *semi-POVM on* Σ^*, which is appropriate for an extension of universal probability.

Definition 1.6 (semi-POVM on Σ^*). *We say $R\colon \Sigma^* \to \mathcal{B}(X)_+$ is a semi-POVM on Σ^* if R satisfies $\sum_{s \in \Sigma^*} R(s) \leqslant I$ where the series converges strongly.*

Obviously, any POVM on Σ^* is a semi-POVM on Σ^*. Let R be a semi-POVM on Σ^*. It is easy to convert R into a POVM on a countably infinite set by appending an appropriate positive operator to R as follows. We fix any one object w which is not in Σ^*. Let $\widetilde{\Omega}_R = \sum_{s \in \Sigma^*} R(s)$. Then $0 \leqslant \widetilde{\Omega}_R \leqslant I$ and $\sum_{s \in \Sigma^*} R(s) + (I - \widetilde{\Omega}_R) = I$. Thus, by setting $\overline{R}(s) = R(s)$ for every $s \in \Sigma^*$ and $\overline{R}(w) = I - \widetilde{\Omega}_R$, we see that $\overline{R}\colon \Sigma^* \cup \{w\} \to \mathcal{B}(X)_+$ is a POVM on countably infinite set $\Sigma^* \cup \{w\}$ in Definition 1.4. Therefore a semi-POVM on Σ^* has a physical meaning in the same way as a POVM on a countably infinite set. Hence, hereafter, we say that a POVM measurement $\mathcal{M}$ is *described* by a semi-POVM R on Σ^* if $\mathcal{M}$ is described by the POVM $\overline{R}$ on countably infinite set $\Sigma^* \cup \{w\}$. Let us consider the quantum measurement described by the R performed upon a quantum system. We then see that if the state of the quantum system is described by an $x \in X$ with $\|x\| = 1$ immediately before the measurement then, for each $s \in \Sigma^*$, the probability that the result s occurs is given by $\langle R(s)x, x\rangle$.

2 Preliminaries

2.1 Notation

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

$\mathbb{N} \equiv \{0, 1, 2, 3, \dots\}$ is the set of natural numbers, and $\mathbb{N}^+$ is the set of positive integers. $\mathbb{Q}$ is the set of rational numbers. $\mathbb{R}$ is the set of real numbers, and $\mathbb{C}$ is the set of complex numbers. $\mathbb{C}_Q$ is the set of the complex numbers in the form of $a + ib$ with $a, b \in \mathbb{Q}$. Let $N \in \mathbb{N}^+$. $\mathrm{Her}(N)$ is the set of $N \times N$ Hermitian matrices. For each $A \in \mathrm{Her}(N)$, the *norm* of A is denoted by $\|A\|$, i.e., $\|A\| = \max\{|\nu| \mid \nu \text{ is an eigenvalue of } A\}$. For each $A, B \in \mathrm{Her}(N)$, we write $A \leqslant B$ if $B - A$ is positive semi-definite. $\mathrm{Her}_{\mathbb{Q}}(N)$ is the set of $N \times N$ Hermitian matrices whose elements are in $\mathbb{C}_Q$.

2.2 Algorithmic information theory

In the following we concisely review some definitions and results of algorithmic information theory [2, 3]. We assume that the reader is familiar with algorithmic information theory in addition to the theory of computable analysis. (See e.g. Chapter 0 of [6] for the treatment of the computability of complex numbers and complex functions on a discrete set.)

$\Sigma^* \equiv \{\lambda, 0, 1, 00, 01, 10, 11, 000, 001, 010, \dots\}$ is the set of finite binary strings where λ denotes the *empty string*, and Σ^* is ordered as indicated. We identify any string in Σ^* with a positive integer in this order. For any $s \in \Sigma^*$, $|s|$ is the *length* of s. A subset S of Σ^* is called a *prefix-free set* if no string in S is a prefix of another string in S.

A *computer* is a partial recursive function $C\colon \Sigma^* \to \Sigma^*$ whose domain of definition is a prefix-free set. For each computer C and each $s \in \Sigma^*$, $H_C(s)$ is defined by $H_C(s) \equiv \min\{\,|p| \mid p \in \Sigma^* \,\&\, C(p) = s\,\}$. A computer U is said to be *optimal* if for each computer C there exists a constant $\mathrm{sim}(C)$ with the following property; if $C(p)$ is defined, then there is a p' for which $U(p') = C(p)$ and $|p'| \leq |p| + \mathrm{sim}(C)$. It is then shown that there exists an optimal computer. We choose any one optimal computer U as the standard one, and define $H(s) \equiv H_U(s)$, which is referred to as the *program-size complexity* of s, the *information content* of s, or the *Kolmogorov complexity* of s.

Let V be any optimal computer. Chaitin's halting probability Ω_V of V is defined by

$$\Omega_V \equiv \sum_{V(p) \text{ is defined}} 2^{-|p|}. \tag{1}$$

For any $\alpha \in (0,1]$, we say that α is *random* if there exists $c \in \mathbb{N}$ such that, for any $n \in \mathbb{N}^+$, $n - c \leq H(\alpha_n)$ where α_n is the first n bits of the base-two expansion of α. Then [2] showed that, for any optimal computer V, Ω_V is random.

The class of computers is equal to the class of functions which are computed by *self-delimiting Turing machines.* A self-delimiting Turing machine is a certain type of deterministic Turing machine which has two tapes, a program (input) tape and a work tape. A self-delimiting Turing machine is called *universal* if it computes an optimal computer. Let M_V be a universal self-delimiting Turing machine which computes an optimal computer V. Then Ω_V is the probability that M_V halts (and outputs some finite binary string) when M_V starts on the program tape filled with an infinite binary string generated by infinitely repeated tosses of a fair coin.

[2] showed that, for any optimal computer V, $2^{-H_V(s)}$ is a universal probability. Therefore we see that, for any universal probability m, $H(s) = -\log_2 m(s) + O(1)$. Thus it is possible to define $H(s)$ as $-\log_2 m(s)$ with any one universal probability m instead of as $H_U(s)$. We can give another characterization of Ω_V also using a universal probability, as seen in the following theorem. In the proof of the theorem, Theorem 6.6 of [1] is used.

Theorem 2.1. *For any $\alpha \in \mathbb{R}$, $\alpha = \sum_{s\in\Sigma^*} m(s)$ for some universal probability m if and only if $\alpha = \Omega_V$ for some optimal computer V.*

In the present paper, we extend a universal probability to a semi-POVM on Σ^*. Thus, Theorem 2.1 suggests that an extension of Ω_V to an operator can be defined as the sum of the POVM elements of such a semi-POVM on Σ^*. Therefore the most important thing is how to extend a universal probability to semi-POVM on Σ^* on a Hilbert space of infinite dimension. We do this first in what follows.

3 Extension of universal probability

In order to extend a universal probability to semi-POVM on Σ^* which operates on an infinite dimensional Hilbert space, we have to develop a theory of computability for points and operators of such a space. We can construct the theory on any concrete Hilbert spaces such as l^2 and $L^2(\mathbb{R}^{3n})$ with $n \in \mathbb{N}^+$. For the purpose of generality, however, we here adopt an axiomatic approach which encompasses a variety of spaces. Thus we consider the notion of *computability structure on a Banach space* which was introduced by [6] in the late 1980s.

3.1 Computability structures on a Banach space

Let X be a complex Banach space with a norm $\|\cdot\|$, and let φ be a nonempty set of sequences in X. We say φ is a *computability structure* on X if the following three axioms; Axiom 3.1, 3.2, and 3.3 hold. A sequence in φ is regarded as a *computable sequence* in X.

Axiom 3.1 (Linear Forms). *Let $\{x_n\}$ and $\{y_n\}$ be in φ, let $\{\alpha_{nk}\}$ and $\{\beta_{nk}\}$ be computable double sequences of complex numbers, and let $d\colon \mathbb{N}^+ \to \mathbb{N}^+$ be a total recursive function. Then the sequence*

$$s_n = \sum_{k=1}^{d(n)} (\alpha_{nk}x_k + \beta_{nk}y_k)$$

is in φ.

For any double sequence $\{x_{nm}\}$ in X, we say $\{x_{nm}\}$ is *computable* with respect to φ if it is mapped to a sequence in φ by any one recursive bijection from $\mathbb{N}^+$ to $\mathbb{N}^+ \times \mathbb{N}^+$. An element $x \in X$ is called *computable* with respect to φ if the sequence $\{x, x, x, \dots\}$ is in φ.

Axiom 3.2 (Limits). *Suppose that a double sequence $\{x_{nm}\}$ in X is computable with respect to φ, $\{y_n\}$ is a sequence in X, and there exists a total recursive function $e\colon \mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{N}^+$ such that $\|x_{ne(n,k)} - y_n\| \leq 2^{-k}$ for all $n, k \in \mathbb{N}^+$. Then $\{y_n\}$ is in φ.*

Axiom 3.3 (Norms). *If $\{x_n\}$ is in φ, then the norms $\{\|x_n\|\}$ form a computable sequence of real numbers.*

We say a sequence $\{e_n\}$ in X is a *generating set* for X or a *basis* for X if the set of all finite linear combinations of the e_n is dense in X.

Definition 3.4. *Let X be a Banach space with a computability structure φ. We say the pair (X, φ) is effectively separable if there exists a sequence*

$\{e_n\}$ in φ which is a generating set for X. Such a sequence $\{e_n\}$ is called an effective generating set for (X, φ) or a computable basis for (X, φ).

Throughout the rest of this paper, we assume that X is an arbitrary complex Hilbert space of infinite dimension with a computability structure φ such that (X, φ) is effectively separable. We choose any one such a computability structure φ on X as the standard one throughout the rest of this paper, and we do not refer to φ hereafter. For example, we will simply say a sequence $\{x_n\}$ is computable instead of saying $\{x_n\}$ is in φ.

We next define the notion of the computability for a semi-POVM on Σ^* as a natural extension of *effectively determined* bounded operator which is defined in [6].

Definition 3.5. *Let R be a semi-POVM on Σ^*. We say R is computable if there exists an effective generating set $\{e_n\}$ for X such that the mapping $(s, n) \longmapsto (R(s))e_n$ is a computable double sequence in X.*

3.2 Universal semi-POVM

We first introduce the notion of *lower-computable semi-POVM* on Σ^*, which is an extension of the notion of lower-computable semi-measure over semi-POVM on Σ^*. The following Definition 3.6 is needed to introduce the notion of lower-computable semi-POVM on Σ^*. We say a basis $\{e_n\}$ for X is *orthonormal* if $\langle e_m, e_n\rangle = \delta_{mn}$ for any $m, n \in \mathbb{N}^+$. As shown in Chapter 4 of [6], we can assume that there exists a computable orthonormal basis for X.

Definition 3.6. *Let $\{e_i\}$ be an orthonormal basis for X. For any $T \in \mathcal{B}(X)$ and $m \in \mathbb{N}^+$, we say T is an m-square operator on $\{e_i\}$ if for all $k, l \in \mathbb{N}^+$ if $k > m$ or $l > m$ then $\langle Te_k, e_l\rangle = 0$. Furthermore, we say T is an m-square rational operator on $\{e_i\}$ if T is an m-square operator on $\{e_i\}$ and for all $k, l \in \mathbb{N}^+$, $\langle Te_k, e_l\rangle \in \mathbb{C}_Q$*

The following Lemma 3.7 is suggestive to fix the definition of lower-computable semi-POVM on Σ^*. By Lemma 3.7, we can effectively check whether $S \leqslant T$ holds or not, given $S, T \in \mathcal{B}_h(X)$ and $m \in \mathbb{N}^+$ such that S and T are m-square operators on an orthonormal basis for X.

Lemma 3.7. *Let $T \in \mathcal{B}_h(X)$, and let $\{e_i\}$ be an orthonormal basis for X. Then, the following two conditions (i) and (ii) are equivalent to each other.*

(i) T is a positive operator.

(ii) For all finite sequence $\nu_1, \dots, \nu_m \in \mathbb{N}^+$ with $\nu_1 < \cdots < \nu_m$,

$$\det\begin{pmatrix} \langle Te_{\nu_1}, e_{\nu_1}\rangle & \cdots & \langle Te_{\nu_1}, e_{\nu_m}\rangle \\ \vdots & & \vdots \\ \langle Te_{\nu_m}, e_{\nu_1}\rangle & \cdots & \langle Te_{\nu_m}, e_{\nu_m}\rangle \end{pmatrix} \geq 0.$$

We recall that, for any lower-computable semi-measure r, there exists a total recursive function $f \colon \mathbb{N}^+ \times \Sigma^* \to \mathbb{Q}$ such that, for each $s \in \Sigma^*$, $\lim_{n\to\infty} f(n, s) = r(s)$ and $\forall n \in \mathbb{N}^+\ 0 \leq f(n, s) \leq f(n+1, s) \leq r(s)$. We here consider how to extend this f to an operator in order to define a lower-computable semi-POVM R on Σ^*. Let $\{e_i\}$ be an orthonormal basis for X. When we prove the existence of universal semi-POVM (i.e., Theorem 3.15), we have to be able to decide whether $f(n, s) \leqslant f(n+1, s)$ in the sequence $\{f(n, s)\}_{n\in\mathbb{N}^+}$ of operators which converges to $R(s)$. Thus, firstly, it is necessary for each $f(s, n)$ to be an m-square rational operator on $\{e_i\}$ for some $m \in \mathbb{N}^+$. If so we can use Lemma 3.7 to check $f(n, s) \leqslant f(n+1, s)$. On that basis, in order to complete the definition of a lower-computable semi-POVM, it seems at first glance that we have only to require that $0 \leqslant f(n, s) \leqslant f(n+1, s) \leqslant R(s)$ and $f(n, s)$ converges to $R(s)$ in an appropriate sense. Note that each operator $f(n, s)$ in the sequence has to be positive in order to guarantee that the limit $R(s)$ is positive. However, this passing idea does not work properly as shown by the following consideration.

For simplicity, we consider matrices in $\mathrm{Her}(N)$ with $N \in \mathbb{N}^+$ instead of operators in X. We show that for some computable matrix $A \geqslant 0$ there does not exist a total recursive function $F \colon \mathbb{N}^+ \to \mathrm{Her}_{\mathbb{Q}}(N)$ such that

$$\lim_{n\to\infty} F(n) = A \text{ and } \forall n \in \mathbb{N}^+\ 0 \leqslant F(n) \leqslant A. \quad (2)$$

This follows from Example 3.9 below, which is based on the following result of linear algebra.

Proposition 3.8. *Let $A, B \in \mathrm{Her}(N)$. Suppose that $\operatorname{rank} A = 1$ and $0 \leqslant B \leqslant A$. Then $B = \tau A$ for some $\tau \in [0, 1]$.*

Example 3.9. *We consider the matrix $A \in \mathrm{Her}(2)$ given by*

$$A = \begin{pmatrix} \frac{2}{3} & \frac{\sqrt{2}}{3} \\ \frac{\sqrt{2}}{3} & \frac{1}{3} \end{pmatrix}.$$

Obviously A is computable. However, since $\operatorname{rank} A = 1$, *by Proposition 3.8 there does not exist any nonzero $B \in \mathrm{Her}_{\mathbb{Q}}(2)$ such that $0 \leqslant B \leqslant A$.*

Thus, even in non-effective manner, we cannot get a sequence $\{F(n)\} \subset \mathrm{Her}_{\mathbb{Q}}(N)$ which satisfies the condition (2). On the other hand, for any positive semi-definite $A \in \mathrm{Her}(N)$ and any $n \in \mathbb{N}^+$, there exists a $B \in \mathrm{Her}_{\mathbb{Q}}(N)$ such that $0 \leqslant B \leqslant A + 2^{-n}E$, where E is the identity matrix. This is because, since $\mathrm{Her}_{\mathbb{Q}}(N)$ is dense in $\mathrm{Her}(N)$ with respect to the norm $\|\cdot\|$, there exists a $B \in \mathrm{Her}_{\mathbb{Q}}(N)$ such that $\|A + 2^{-n+1}/3E - B\| \leq 2^{-n}/3$. Thus we have $0 \leqslant A + 2^{-n}/3E \leqslant B \leqslant A + 2^{-n}E$. Furthermore we can show that, for any positive semi-definite $A \in \mathrm{Her}(N)$, if A is computable, then there exists a total recursive function $F \colon \mathbb{N}^+ \to \mathrm{Her}_{\mathbb{Q}}(N)$ such that (i) $\lim_{n\to\infty} F(n) = A$, (ii) $0 \leqslant F(n)$, and (iii) $F(n) - 2^{-n}E \leqslant F(n+1) - 2^{-(n+1)}E \leqslant A$. Note that a positive semi-definite matrix A with rank 1 as considered in Example 3.9 is not an atypical example as a POVM elements, since such a POVM element is common in a familiar projective measurement.

The foregoing consideration suggests the following definition of a lower-computable semi-POVM on an infinite dimensional Hilbert space.

Definition 3.10. *Let $\{e_i\}$ be a computable orthonormal basis for X, and let R be a semi-POVM on Σ^*. We say R is lower-computable with respect to $\{e_i\}$ if there exist an $f \colon \mathbb{N}^+ \times \Sigma^* \to \mathcal{B}(X)_+$ and a total recursive function $g \colon \mathbb{N}^+ \times \Sigma^* \to \mathbb{N}^+$ such that*

(i) for each $s \in \Sigma^*$, $f(n, s)$ converges strongly to $R(s)$ as $n \to \infty$,

(ii) for all n and s, $f(n, s) - 2^{-n}I \leqslant f(n+1, s) - 2^{-(n+1)}I$,

(iii) for all n and s, $f(n, s)$ is a $g(n, s)$-square rational operator on $\{e_i\}$, and

(iv) the mapping $\mathbb{N}^+ \times \Sigma^* \times \mathbb{N}^+ \times \mathbb{N}^+ \ni (n, s, i, j) \longmapsto \langle f(n, s)e_i, e_j\rangle$ is a total recursive function.

In the above definition, we choose the sequence $\{2^{-n}\}$ as the coefficients of I in the inequality of the condition (ii). Note, however, that in the definition we can equivalently replace $\{2^{-n}\}$ by any recursive nonincreasing sequence of non-negative rational numbers which converges to 0.

We can show that the lower-computability of semi-POVM on Σ^* given in Definition 3.10 does not depend on the choice of a computable orthonormal basis used in the definition. This fact is verified using the following Lemma 3.11, which follows from Lemma 3.7.

Lemma 3.11. *Let $T \in \mathcal{B}_h(X)$ be an m-square operator on an orthonormal basis $\{e_i\}$ for X. For any real number $a > 0$, $0 \leqslant T + aI$ if and only if $0 \leqslant T + aI_m$ where I_m is the operator in $\mathcal{B}_h(X)$ such that $I_m e_i = e_i$ if $i \leq m$ and $I_m e_i = 0$ otherwise.*

By Lemma 3.11, in order to check whether the condition (ii) of Definition 3.10 holds, we can equivalently check the condition that $0 \leqslant f(n+1, s) - f(n, s) + 2^{-n-1}I_m$ if $f(n, s)$ and $f(n+1, s)$ are m-square operators on an orthonormal basis $\{e_i\}$ for X.

Thus, we define the notion of a lower-computable semi-POVM on Σ^* independently of a choice of a computable orthonormal basis for X.

Definition 3.12. *Let R be a semi-POVM on Σ^*. We say R is lower-computable if there exists a computable orthonormal basis $\{e_i\}$ for X such that R is lower-computable with respect to $\{e_i\}$.*

Any computable function $r \colon \Sigma^* \to [0, 1]$ with $\sum_{s \in \Sigma^*} r(s) \leq 1$ is shown to be a lower-computable semi-measure. Corresponding to this fact we can show Theorem 3.13 below. For each $T \in \mathcal{B}(X)$, we define $\|T\|_2$ as $(\sum_{i=1}^{\infty} \|Te_i\|^2)^{1/2} \in [0, \infty]$, where $\{e_n\}$ is an arbitrary orthonormal basis for X.

Theorem 3.13. *Suppose that (i) $R \colon \Sigma^* \to \mathcal{B}(X)$ is a computable semi-POVM on Σ^*, (ii) $R(s)$ is Hilbert-Schmidt for every $s \in \Sigma^*$, and (iii) $\{\|R(s)\|_2\}_{s \in \Sigma^*}$ is a computable sequence of real numbers. Then R is lower-computable.*

As a natural generalization of universal probability, the notion of universal semi-POVM is defined as follows.

Definition 3.14 (universal semi-POVM). *Let M be a lower-computable semi-POVM on Σ^*. We say that M is a universal semi-POVM if for each lower-computable semi-POVM R on Σ^*, there exists a real number $c > 0$ such that, for all $s \in \Sigma^*$, $cR(s) \leqslant M(s)$.*

Most importantly we can prove the existence of universal semi-POVM.

Theorem 3.15. *There exists a universal semi-POVM.*

4 Extension of Chaitin's Ω

Now, based on the intuition obtained from Theorem 2.1, we propose to define an extension $\hat{\Omega}$ of Chaitin's Ω as follows.

Definition 4.1 (extension of Ω to operator). *For each universal semi-POVM M, $\hat{\Omega}_M$ is defined by $\hat{\Omega}_M \equiv \sum_{s\in\Sigma^*} M(s)$.*

Let M be a universal semi-POVM. Then, obviously, $\hat{\Omega}_M \in \mathcal{B}(X)_+$ and $\hat{\Omega}_M \leqslant I$. We can further show that $cI \leqslant \hat{\Omega}_M$ for some real number $c > 0$. We can show the following theorem, which supports the above proposal.

Theorem 4.2. *Let M be a universal semi-POVM. If x is a computable point in X with $\|x\| = 1$, then (i) there exists an optimal computer V such that $\left\langle \hat{\Omega}_M x, x \right\rangle = \Omega_V$, and (ii) $\left\langle \hat{\Omega}_M x, x \right\rangle$ is a random real number.*

Let M be any universal semi-POVM, and let x be any point in X with $\|x\| = 1$. Consider the POVM measurement $\mathcal{M}$ described by the M. This measurement produces one of countably many outcomes; elements in Σ^* and one more something which corresponds to the POVM element $I - \Omega_M$. If the measurement $\mathcal{M}$ is performed upon the state described by the x immediately before the measurement, then the probability that a result $s \in \Sigma^*$ occurs is given by $\langle M(s)x, x\rangle$. Therefore $\left\langle \hat{\Omega}_M x, x \right\rangle$ is the probability of getting some finite binary string as a measurement outcome in $\mathcal{M}$.

Now, assume that x is computable. Recall that, for any optimal computer V, Ω_V is the probability that V halts and outputs some finite string, which results from infinitely repeated tosses of a fair coin. Thus, by Theorem 4.2, $\left\langle \hat{\Omega}_M x, x \right\rangle$ has a meaning of classical probability that a universal self-delimiting Turing machine generates some finite string. Hence $\left\langle \hat{\Omega}_M x, x \right\rangle$ has a meaning of probability of producing some finite string in the contexts of both quantum mechanics and algorithmic information theory. Thus, in the case where x is computable, algorithmic information theory is consistent with quantum mechanics in a certain sense.

5 Concluding remarks

Based on the universal semi-POVM, we have introduced $\hat{\Omega}_M$ which is an extension of Chaitin's Ω_U to a measurement operator in infinite dimensional quantum system. In algorithmic information theory, however, Ω_U is originally defined through (1) as the halting probability of the universal self-delimiting Turing machine which computes U. Thus Ω_U is directly related to a behavior of a computing machine. Therefore, in order to develop our operator version of algorithmic information theory further, it is necessary to find more concrete definition of $\hat{\Omega}_M$ which is immediately based on a behavior of some sort of computing machine. We leave the identification of such a machine to a future study.

The author is grateful to the 21st Century COE Program of Chuo University for the financial support.

References

[1] C. S. Calude, P. H. Hertling, B. Khoussainov, and Y. Wang, Recursively enumerable reals and Chaitin Ω numbers. Theoret. Comput. Sci. **255**, 125–149 (2001).

[2] G. J. Chaitin, A theory of program size formally identical to information theory. J. Assoc. Comput. Mach. **22**, 329–340 (1975).

[3] G. J. Chaitin, Incompleteness theorems for random reals. Adv. in Appl. Math. **8**, 119–146 (1987).

[4] P. Gács, Quantum algorithmic entropy. J. Phys. A: Math. Gen. **34**, 6859–6880 (2001).

[5] A. S. Holevo, Statistical Structure of Quantum Theory (Springer-Verlag, Berlin 2001).

[6] M. B. Pour-El and J. I. Richards, Computability in Analysis and Physics. Perspectives in Mathematical Logic (Springer-Verlag, Berlin 1989).

[7] K. Tadaki, A generalization of Chaitin's halting probability Ω and halting self-similar sets. Hokkaido Math. J. **31**, 219–253 (2002). Electronic version available at URL: `http://arxiv.org/abs/nlin/0212001`.

[8] K. Tadaki, Upper bound by Kolmogorov complexity for the probability in computable quantum measurement. In: Proceedings 5th Conference on Real Numbers and Computers (RNC'5), Lyon, France, September 3–5, 2003, pp. 193–214.