Entropy **2011**, *13*, 778-789; doi:10.3390/e13040778

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

Quantum Kolmogorov Complexity and Information-Disturbance Theorem

Takayuki Miyadera

Research Center for Information Security, National Institute of Advanced Industrial Science and Technology, Daibiru building 1003, Sotokanda, Chiyoda-ku, Tokyo, 101-0021, Japan;
E-Mail: miyadera-takayuki@aist.go.jp; Tel.: +81-3-5298-4722, Fax: +81-3-5298-4522

Received: 17 January 2011; in revised form: 9 March 2011 / Accepted: 24 March 2011 / Published: 29 March 2011

Abstract: In this paper, a representation of the information-disturbance theorem based on the quantum Kolmogorov complexity that was defined by P. Vitányi has been examined. In the quantum information theory, the information-disturbance relationship, which treats the trade-off relationship between information gain and its caused disturbance, is a fundamental result that is related to Heisenberg's uncertainty principle. The problem was formulated in a cryptographic setting and the quantitative relationships between complexities have been derived.

Keywords: quantum Kolmogorov complexity; information-disturbance theorem; uncertainty principle

1. Introduction

The quantum theory enables us to process information in ways that are not feasible in the classical world. Quantum computers can solve difficult problems such as factoring [1] or searching [2] in drastically small time steps. Quantum key distribution [3,4] achieves information-theoretic security unconditionally. This field of the quantum information theory has been intensively studied during the last two decades. While most of the studies in this field investigate how Shannon's information theory was modified or restricted by the quantum theory, there is another information theory called the algorithmic information theory [5,6]. In contrast to Shannon's theory, which defines information using a probability distribution, the algorithmic information theory assigns the concept of information to individual objects by using a computation theory. Although the algorithmic information theory has been successfully applied to various fields [7], its quantum versions were only recently proposed [8–11]. We believe there have only been a few applications so far [12–14]. In this research, we study how quantum Kolmogorov complexity, which was defined by Vitányi, can be applied to demonstrate quantum effects in a primitive information-theoretic operation.

We study the algorithmic information-theoretic representation of an information-disturbance relationship [15–17], which addresses a fundamental observation that information gain destroys quantum states. In particular, an operation that yields information gain with respect to an observable spoils quantum states that were prepared with respect to its conjugate (noncommutative) observable. This relationship indicates the impossibility of jointly measuring noncommutative observables, which is therefore related to Heisenberg's uncertainty principle. In addition, it plays a crucial role in quantum cryptography. Because a state is inevitably spoiled when an eavesdropper obtains information, legitimate users can notice the existence of the eavesdropper [18]. In this study, we formulate the problem in a cryptographic setting and derive quantitative relationships. Our theorem, characterizing both the information gain and the disturbance in terms of the quantum Kolmogorov complexity, demonstrates a trade-off relationship between these complexities.

This paper is organized as follows. In the next section, we give a brief review of quantum Kolmogorov complexity defined by Vitányi. In Section 3, we introduce a toy quantum cryptographic model and describe our main result on the basis of this model. The paper ends a short discussion.

2. Quantum Kolmogorov Complexity Based on Classical Description

Recently some quantum versions of Kolmogorov complexity were proposed by a several researchers. Svozil [9], in his pioneering work, defined the quantum Kolmogorov complexity as the minimum classical description length of a quantum state through a quantum Turing machine [19,20]. As is easily seen by comparing the cardinality of a set of all the programs with that of a set of all the quantum states, the value often becomes infinity. Vitányi's definition [8], while similar to Svozil's, does not have this disadvantage. Vitányi added a term that compensates for the difference between a target state and an output state. Berthiaume, van Dam and Laplante [10] defined their quantum Kolmogorov complexity as the length of the shortest quantum program that outputs a target state. The definition was settled and its properties were extensively investigated by Müller [21,22]. Gacs [11] employed a different starting point related to the algorithmic probability to define his quantum Kolmogorov complexity.

In this paper we employ a definition given by Vitányi [8]. His definition based on the classical description length is suitable for quantum information-theoretic problems which normally treat classical inputs and outputs. In order to explain the definition precisely, a description of one-way quantum Turing machine is needed. It is utilized to define a prefix quantum Kolmogorov complexity. A one-way quantum Turing machine consists of four tapes and an internal control. (See [8] for more details.) Each tape is a one-way infinite qubit (quantum bit) chain and has a corresponding head on it. One of the tapes works as the input tape and is read-only from left-to-right. A program is given on this tape as an initial condition. The second tape works as the work tape. The work tape is initially set to be 0 for all the cells. The head on it can read and write a cell and can move in both directions. The third tape is called an auxiliary tape. One can put an additional input on this tape. The additional input is written to the leftmost qubits and can be a quantum state or a classical state. This input is needed when one treats conditional Kolmogorov complexity. The fourth tape works as the output tape. It is assumed that after halting the state over this tape will not be changed. The internal control is a quantum system described by a finite dimensional Hilbert space which has two special orthogonal vectors $|q_0\rangle$ (initial state) and $|q_f\rangle$ (halting state). After each step one makes a measurement of a coarse grained observable on the internal control $\{|q_f\rangle\langle q_f|, \mathbf{1} - |q_f\rangle\langle q_f|\}$ to know if the computation halts. Although there are subtle problems [23–26] in the halting process of the quantum Turing machine, we do not get into this problem and employ a simple definition of the halting. A computation halts at time t if and only if the probability to observe q_f at time t is 1, and at any time $t' < t$ the probability to observe q_f is zero. By using this one-way quantum Turing machine, Vitányi defined the quantum Kolmogorov complexity as the length of the shortest description of a quantum state. That is, the programs of quantum Turing machine are restricted to classical ones, while the auxiliary inputs can be quantum states. We write $U(p, y) = |x\rangle$ if and only if a quantum Turing machine U with a classical program p and an auxiliary (classical or quantum) input y halts and outputs $|x\rangle$. The following is the precise description of Vitányi's definition.

Definition 1 *[8] The (self-delimiting) quantum Kolmogorov complexity of a pure state $|x\rangle$ with respect to a one-way quantum Turing machine U with y (possibly a quantum state) as conditional input given for free is*

$$K_U(|x\rangle|\, y) := \min_{p,|z\rangle}\{l(p) + \lceil -\log|\langle z|x\rangle|^2\rceil : U(p, y) = |z\rangle\}$$

where $l(p)$ is the length of a classical program p, and $\lceil a \rceil$ is the smallest integer larger than a.

The one-wayness of the quantum Turing machine ensures that the halting programs compose a prefix free set. Because of this, the length $l(p)$ is defined consistently. The term $\lceil -\log|\langle z|x\rangle|^2\rceil$ represents how insufficiently an output $|z\rangle$ approximates the desired output $|x\rangle$. This additional term has a natural interpretation using the Shannon-Fano code. Vitányi has shown the following invariance theorem, which is very important.

Theorem 1 *[8] There is a universal quantum Turing machine U, such that for all machines Q, there is a constant c_Q, such that for all quantum states $|x\rangle$ and all auxiliary inputs y we have:*

$$K_U(|x\rangle|\, y) \leq K_Q(|x\rangle|\, y) + c_Q$$

Thus the value of quantum Kolmogorov complexity does not depend on the choice of a quantum Turing machine if one neglects the unimportant constant term c_Q. Thanks to this theorem, one often writes K instead of K_U. Moreover, the following theorem is crucial for our discussion.

Theorem 2 *[8] On classical objects (that is, finite binary strings that are all directly computable) the quantum Kolmogorov complexity coincides up to a fixed additional constant with the self-delimiting Kolmogorov complexity. That is, there exists a constant c such that for any classical binary sequence $|x\rangle$,*

$$\min_q\{l(q) : U(q, y) = |x\rangle\} \geq K(|x\rangle|\, y) \geq \min_q\{l(q) : U(q, y) = |x\rangle\} - c$$

holds.

According to this theorem, for classical objects it essentially suffices to treat only programs that exactly output the object.

3. Information-Disturbance Trade-Off

In this section, we treat a toy model of quantum key distribution in order to discuss the information-disturbance relationship. Let us first review a standard scenario of quantum key distribution called BB84. Suppose that there exist three players Alice, Bob, and Eve. Alice and Bob are legitimate users. Alice encodes a message in qubits with one of the bases X or Z, and sends them to Bob. After confirming the receipt of the qubits by Bob, she announces the basis that was used by her for encoding. If there is no eavesdropper, Bob can perfectly recover the message by simply measuring the qubits by using the disclosed basis. Conversely, if there exists an eavesdropper Eve, the state received by Bob is destroyed and he will be unable to recover the message in that case. More precisely, according to the information-disturbance theorem in Shannon's information-theoretical representation, Bob's state is inevitably spoiled when Eve employs an attack that helps her obtain information about the messages encoded in the conjugate basis. In order to accomplish the key distribution protocol, Alice and Bob perform an error correction followed by a privacy amplification.

Motivated by this protocol, we introduce its toy version in order to investigate a universal relationship between information gain and disturbance. There are three players Alice, Bob and Eve. Alice chooses an N-bit message $y \in \{0,1\}^N$ and a basis X or Z for its encoding. We write the standard basis of a qubit as $\{|0\rangle, |1\rangle\}$, which are eigenstates of Z. Its conjugate basis is written as $\{|\overline{0}\rangle, |\overline{1}\rangle\}$, which are eigenstates of X and are defined as $|\overline{0}\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\overline{1}\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. She prepares a quantum state of N qubits described by a Hilbert space $\mathcal{H}_A := \mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \cdots \otimes \mathbf{C}^2$ (N times) as follows. If her choice of basis is X, she encodes her message $y = y_1 y_2 \cdots y_N \in \{0,1\}^N$ as $|\overline{y}\rangle := |\overline{y_1}\rangle \otimes |\overline{y_2}\rangle \otimes \cdots \otimes |\overline{y_N}\rangle \in \mathcal{H}_A$. If her choice of basis is Z, she encodes her message y as $|y\rangle := |y_1\rangle \otimes |y_2\rangle \otimes \cdots \otimes |y_N\rangle \in \mathcal{H}_A$. Alice sends thus prepared N qubits to Bob. Eve, whose purpose is to obtain information about the message, makes her apparatus interact with the qubits sent from Alice to Bob and divides the whole system into two parts. This process is described by a completely-positive map (CP-map)

$$\Lambda : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B \otimes \mathcal{H}_E)$$

where $\mathcal{H}_B$ (resp. $\mathcal{H}_E$) denotes a Hilbert space of the system distributed to Bob (resp. Eve), and $\mathcal{S}(\mathcal{H})$ is a set of all density operators on a Hilbert space $\mathcal{H}$. Alice then announces the basis X or Z that she had used for encoding. Bob and Eve try estimating the message by using the quantum state and the information of the basis. Note that in this protocol $\mathcal{H}_B$ and $\mathcal{H}_E$ may be general quantum systems. In particular, $\mathcal{H}_B$ may not be qubits. Thus in contrast to the standard quantum key distribution protocol, Bob may not measure X or Z to obtain information. Bob knows the basis used for encoding and the form of CP-map Λ. Thus Bob and Eve are equal in their knowledge on classical information. Only the distributed quantum states differ with each other. According to the information-disturbance relationship in Shannon's information-theoretical setting, if Eve's attack helps her obtain large information about the message encoded in the X basis, Bob cannot obtain large information about the message encoded in the Z basis. If the message is chosen probabilistically [27], this relationship is expressed in the formula as [17]:

$$I(A:E|\text{basis} = X) + I(A:B|\text{basis} = Z) \leq N$$

where A represents the random variable of the message and E (resp. B) represents the random variable of the outcome of the measurement performed by Eve (resp. Bob), and $I(\cdot,\cdot)$ denotes Shannon's mutual information.

We formulate the above problem in the algorithmic information-theoretical setting. Let us denote the quantum state obtained by Bob (resp. Eve) corresponding to the message z (resp. x) encoded with the basis Z (resp. X) by $\rho_z^B \in \mathcal{S}(\mathcal{H}_B)$ (resp. $\sigma_x^E \in \mathcal{S}(\mathcal{H}_E)$). That is, ρ_z^B and σ_x^E are defined by

$$\begin{aligned}\rho_z^B &= \mathrm{tr}_{\mathcal{H}_E}(\Lambda(|z\rangle\langle z|))\\ \sigma_x^E &= \mathrm{tr}_{\mathcal{H}_B}(\Lambda(|\overline{x}\rangle\langle\overline{x}|))\end{aligned}$$

where $\mathrm{tr}_{\mathcal{H}_E}$ (resp. $\mathrm{tr}_{\mathcal{H}_B}$) denotes a partial trace over $\mathcal{H}_E$ (resp. $\mathcal{H}_B$). Motivated by the above result in Shannon's formulation, we expect that there will exist some trade-off relationship between $K(x|\sigma_x^E, X)$ and $K(z|\rho_z^B, Z)$ [28]. $K(x|\sigma_x^E, X)$ is the quantum Kolmogorov complexity of the message x encoded with X for Eve. Note that Eve has quantum state σ_x^E, and knows X (and Λ). $K(z|\rho_z^B, Z)$ is the quantum Kolmogorov complexity of the message z encoded with Z for Bob. He has quantum state ρ_z^B, and knows Z (and Λ). The following is our main theorem.

Theorem 3 *There exists a trade-off relationship for the number of messages that have low complexity. For any integers $l, m \geq 0$,*

$$\left|\{z|K(z|\rho_z^B, Z) \leq l\}\right| + \left|\{x|K(x|\sigma_x^E, X) \leq m\}\right| \leq 2^N \left(1 + 2^{\frac{l+m-N}{2}+c}\right)$$

holds, where $|A|$ denotes the cardinality of a set A and c is a constant depending on the choice of the quantum Turing machine. Note that the right-hand side of the above inequality gives a nontrivial bound for l, m satisfying $l + m \leq N - 2c$.

Proof: The proof has three parts. (i) An entanglement-based protocol which is related to the original one is introduced. (ii) It is shown that the number of messages that have low complexity can be represented by an expectation value of a certain observable in the entanglement-based protocol. (iii) The uncertainty relation is applied to show a trade-off relationship.

(i) Let us analyze the protocol. Instead of the original protocol, we treat an entanglement-based protocol (E91-like protocol), which is related to the original one. It runs as follows. Alice prepares N pairs of qubits. She prepares each pair in the EPR state, $|\phi\rangle := \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$. Therefore, the whole state can be written as $|\phi^N\rangle := |\phi\rangle \otimes |\phi\rangle \otimes \cdots \otimes |\phi\rangle$ (N times) in a Hilbert space $\mathcal{H}_{A'} \otimes \mathcal{H}_A$, where $\mathcal{H}_{A'} \simeq \mathcal{H}_A \simeq \otimes^N \mathbf{C}^2$. Alice sends qubits described by $\mathcal{H}_A$ to Bob. Before the qubits reach Bob, Eve makes them interact with her own apparatus, and divides the whole system into two parts. The whole dynamics is described by $(\mathrm{id}_{\mathcal{S}(\mathcal{H}_{A'})} \otimes \Lambda) : \mathcal{S}(\mathcal{H}_{A'} \otimes \mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_{A'} \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$, where $\mathrm{id}_{\mathcal{S}(\mathcal{H}_{A'})}$ is an identity map on $\mathcal{S}(\mathcal{H}_{A'})$. We denote by Θ the whole state over $\mathcal{H}_{A'} \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ after this process. That is, it is defined by $\Theta = (\mathrm{id}_{\mathcal{H}_{A'}} \otimes \Lambda)(|\phi^N\rangle\langle\phi^N|)$. Alice then measures her qubits with the basis X or Z, and announces the basis used.

It can be shown [17] that this entanglement-based protocol is equivalent with the original protocol with a probabilistically [27] chosen message. In fact, we can see the following correspondence. Define Z_z for $z \in \{0,1\}^N$, a projection operator on $\mathcal{H}_{A'}$, by $Z_z := |z\rangle\langle z|$. $\{Z_z\}$ forms a projection-valued measure (PVM). Probability to obtain $z \in \{0,1\}^N$ in its measurement is $P_Z(z) := \mathrm{tr}(\Theta(Z_z \otimes \mathbf{1}_B \otimes$

$\mathbf{1}_E)) = \frac{1}{2^N}$. In addition, *a posteriori* state [29] on $\mathcal{H}_B \otimes \mathcal{H}_E$ is calculated as $\Lambda(|z\rangle\langle z|)$, whose restriction on $\mathcal{H}_B$ is nothing but $\rho_z^B \in \mathcal{S}(\mathcal{H}_B)$. Similarly, define X_x for $x \in \{0,1\}^N$, a projection operator on $\mathcal{H}_{A'}$, by $X_x = |\overline{x}\rangle\langle\overline{x}|$. It is easy to see that $\{X_x\}_{x\in\{0,1\}^N}$ forms a PVM on $\mathcal{H}_{A'}$. For each $x \in \{0,1\}^N$, probability to obtain x in its measurement is $P_X(x) = \frac{1}{2^N}$. *A posteriori* state [29] on $\mathcal{H}_B \otimes \mathcal{H}_E$ becomes $\Lambda(|\overline{x}\rangle\langle\overline{x}|)$, whose restriction on $\mathcal{H}_E$ is σ_x^E.

(ii) We fix a universal quantum Turing machine U and discuss the quantum Kolmogorov complexity with respect to it. Firstly let us consider the complexity for Bob when the message z is encoded with Z. Bob knows Z and has a quantum system described by $\mathcal{H}_B$ whose state is ρ_z^B. This system is identified with the auxiliary input tape. That is, we investigate $K_U(z|\rho_z^B, Z)$. Thanks to theorem 2, it suffices to consider only the programs that exactly output the message z because the message is a classical object. That is, we regard

$$K_{c,U}(z|\rho_z^B, Z) := \min_{q:U(q,\rho_z^B,Z)=|z\rangle} l(q)$$

which satisfies $K_{c,U}(z|\rho_z^B, Z) \geq K_U(z|\rho_z^B, Z) \geq K_{c,U}(z|\rho_z^B, Z) - c'$ for some constant c'.

Let us denote $T_z \subset \{0,1\}^*$ a set of all programs that output z with auxiliary inputs ρ_z^B and Z. A relationship $K_{c,U}(z|\rho_z^B, Z) = \min_{t\in T_z} l(t)$ follows. Although different programs may have different halting times, thanks to the lemma proved by Müller (Lemma 2.3.4. in [22]), there exists a CP-map $\Gamma_{U,Z} : \mathcal{S}(\mathcal{H}_B \otimes \mathcal{H}_I) \to \mathcal{S}(\mathcal{H}_O)$ satisfying for any $t \in T_z$

$$\Gamma_{U,Z}(\rho_z^B \otimes |t\rangle\langle t|) = |z\rangle\langle z|$$

where $\mathcal{H}_I$ is a Hilbert space for programs, and $\mathcal{H}_O = \otimes^N \mathbf{C}_2$ is a Hilbert space for outputs. From this lemma, we obtain an important observation. If $T_z \cap T_{z'} \neq \emptyset$ holds for some $z \neq z'$, ρ_z^B and $\rho_{z'}^B$ are perfectly distinguishable. In fact, as a CP-map does not increase the distinguishability of states, the relationships for $t \in T_z \cap T_{z'}$

$$\begin{aligned} \Gamma_{U,Z}(\rho_z^B \otimes |t\rangle\langle t|) &= |z\rangle\langle z| \\ \Gamma_{U,Z}(\rho_{z'}^B \otimes |t\rangle\langle t|) &= |z'\rangle\langle z'| \end{aligned}$$

and their distinguishability on the right-hand sides imply the distinguishability of ρ_z^B and $\rho_{z'}^B$. For each $t \in \{0,1\}^*$ we define $\mathcal{C}_t \subset \{0,1\}^N$ as $\mathcal{C}_t = \{z | t \in T_z\}$. That is, $z \in \mathcal{C}_t$ is a message which can be reconstructed by giving a program t to the Turing machine U with an auxiliary input ρ_z^B and Z. Owing to the distinguishability between ρ_z^B and $\rho_{z'}^B$, for $z, z' \in \mathcal{C}_t$, there exists a family of projection operators $\{E_z^t\}_{z\in\mathcal{C}_t}$ on $\mathcal{H}_B$ satisfying for any $z, z' \in \mathcal{C}_t$,

$$\begin{aligned} &E_z^t E_{z'}^t = \delta_{zz'} E_z^t \\ &\sum_{z\in\mathcal{C}_t} E_z^t \leq \mathbf{1} \\ &\mathrm{tr}(\rho_z^B E_{z'}^t) = \delta_{zz'} \end{aligned}$$

As we are interested in minimum length programs, we define $\mathcal{D}_t := \{z | t = \mathrm{argmin}_{s\in T_z} l(s)\}$, which is a subset of $\mathcal{C}_t$. $z \in \mathcal{D}_t$ is a message that has t as its minimum length program for reconstruction. It is still possible that $\mathcal{D}_t \cap \mathcal{D}_{t'} \neq \emptyset$. That is, there may be a message z whose shortest programs are not unique. In such a case, we choose one of the programs to avoid counting doubly. For instance, this can be done by introducing a total order $<$ in all the programs $\{0,1\}^*$, and by defining $\mathcal{E}_t = \{z|z \in \mathcal{D}_t, z \notin \mathcal{D}_{t'}$ for all $t' < t$ with $l(t) = l(t')\}$. As this $\mathcal{E}_t$ is a subset of $\mathcal{C}_t$, for any $z, z' \in \mathcal{E}_t$

$$
\begin{aligned}
&E_z^t E_{z'}^t = \delta_{zz'} E_z^t \\
&\sum_{z \in \mathcal{E}_t} E_z^t \leq \mathbf{1} \\
&\mathrm{tr}(\rho_z^B E_{z'}^t) = \delta_{zz'}
\end{aligned}
$$

hold.

For any program $t \in \{0,1\}^*$ we define a projection operator $P_t := \sum_{z \in \mathcal{E}_t} (Z_z \otimes E_z^t \otimes \mathbf{1}_E)$. For any integer $l \geq 0$, we consider a projection operator $\hat{P}_l := \sum_{t:l(t) \leq l} P_t$, whose expectation value with Θ becomes

$$
\begin{aligned}
\mathrm{tr}(\Theta \hat{P}_l) &= \sum_{t:l(t) \leq l} \sum_{z \in \mathcal{E}_t} P_Z(z) \mathrm{tr}(\rho_z^B E_z^t) \\
&= \sum_{t:l(t) \leq l} \sum_{z \in \mathcal{E}_t} P_Z(z) \\
&= \frac{1}{2^N} \left| \{z | K_{c,U}(z|\rho_z^B, Z) \leq l\} \right| \qquad (1)
\end{aligned}
$$

Similarly, we treat $K_{c,U}(x|\sigma_x^E, X)$. We can introduce $S_x \subset \{0,1\}^*$ a set of all programs that output x with auxiliary inputs σ_x^E and X. $K_{c,U}(x|\sigma_x^E, X) = \min_{s \in S_x} l(s)$ holds. We can define $\mathcal{J}_s := \{x|s \in S_x\}$ for each s and introduce a family of projection operators $\{F_x^s\}_{x \in \mathcal{F}_s}$ on $\mathcal{H}_E$ that satisfies

$$
\mathrm{tr}(F_x^s \sigma_{x'}^E) = \delta_{xx'}
$$

for each $x, x' \in \mathcal{J}_s$ and so on. $\mathcal{G}_s := \{x|s = \mathrm{argmin}_{t \in S_x} l(t)\}$ and $\mathcal{F}_s := \{z|z \in \mathcal{G}_s, z \notin \mathcal{G}_{s'}$ for all $s' < s$ with $l(s) = l(s')\}$, are also defined. We consider a family of projection operators $\{F_x^s\}_{x \in \mathcal{F}_s}$. Similarly, for any program $s \in \{0,1\}^*$, we define a projection operator $Q_s := \sum_{x \in \mathcal{F}_s} (X_x \otimes \mathbf{1}_B \otimes F_x^s)$ and consider for any integer $m \geq 0$, $\hat{Q}_m := \sum_{s:l(s) \leq m} Q_s$, whose expectation value with respect to Θ is written as

$$
\mathrm{tr}(\Theta \hat{Q}_m) = \frac{1}{2^N} \left| \{x | K_{c,U}(x|\sigma_x^E, X) \leq m\} \right| \qquad (2)
$$

(iii) Our purpose is to obtain a trade-off relationship between (1) and (2). It is obtained by applying the uncertainty relation, which is often regarded as the most fundamental inequality characterizing quantum mechanics. Among the various forms of the uncertainty relation, we employ the Landau-Pollak uncertainty relation for arbitrary numbers of projection operators [30]. For a finite family of projection operators $\{A_i\}$ and any state ρ, it holds that

$$
\sum_i \mathrm{tr}(\rho A_i) \leq 1 + \left(\sum_{i \neq j} \|A_i A_j\|^2 \right)^{1/2}
$$

We apply this inequality for a family of projection operators $\{P_t, Q_s\}$ $(l(t) \leq l, l(s) \leq m)$ and the state Θ. As $P_t P_{t'} = 0$ for $t \neq t'$ and $Q_s Q_{s'} = 0$ for $s \neq s'$ hold thanks to $\mathcal{E}_t \cap \mathcal{E}_{t'} = \mathcal{F}_s \cap \mathcal{F}_{s'} = \emptyset$, we obtain

$$
\mathrm{tr}(\Theta \hat{P}_l) + \mathrm{tr}(\Theta \hat{Q}_m) \leq 1 + \left(2 \sum_t^{l(t) \leq l} \sum_s^{l(s) \leq m} \|P_t Q_s\|^2 \right)^{1/2}
$$

The term $\|P_tQ_s\|$ of the right-hand side is computed as follows. As the operator norm $\|P_tQ_s\|$ is written as $\|P_tQ_s\| = \sup_{|\Psi\rangle:\||\Psi\rangle\|=1} \|P_tQ_s|\Psi\rangle\|$, we need to bound $\|P_tQ_s|\Psi\rangle\|$ for any normalized vector $|\Psi\rangle$.

$$\begin{aligned}
\|\sum_{z\in\mathcal{E}_t}\sum_{x\in\mathcal{F}_s}(Z_zX_x\otimes E^t_z\otimes F^s_x)|\Psi\rangle\| &= \left(\sum_{z\in\mathcal{E}_t}\sum_{x\in\mathcal{F}_s}\langle\Psi|(X_xZ_zX_x\otimes E^t_z\otimes F^s_x)|\Psi\rangle\right)^{1/2} \\
&= \left(\sum_{z\in\mathcal{E}_t}\sum_{x\in\mathcal{F}_s}\mathrm{tr}(\mu^{t,s}_{z,x}X_xZ_zX_x)\langle\Psi|\mathbf{1}_A\otimes E^t_z\otimes F^s_x|\Psi\rangle\right)^{1/2}
\end{aligned}$$

where we used $E^t_zE^t_{z'} = 0$ for $z \neq z'$ and $F^s_xF^s_{x'} = 0$ for $x \neq x'$, and $\mu^{t,s}_{z,x}$ is *a posteriori* state [29] defined as a unique state satisfying the above equality.
As $|\mathrm{tr}(\mu^{t,s}_{z,x}X_xZ_zX_x)| \leq \|X_xZ_zX_x\| = \frac{1}{2^N}$ holds, we obtain

$$\begin{aligned}
\left(\sum_{z\in\mathcal{E}_t}\sum_{x\in\mathcal{F}_s}\mathrm{tr}(\mu^{t,s}_{z,x}X_xZ_zX_x)\langle\Psi|\mathbf{1}_A\otimes E^t_z\otimes F^s_x|\Psi\rangle\right)^{1/2} &\leq \frac{1}{2^{N/2}}\left(\sum_{z\in\mathcal{E}_t}\sum_{x\in\mathcal{F}_s}\langle\Psi|\mathbf{1}_A\otimes E^t_z\otimes F^s_x|\Psi\rangle\right)^{1/2} \\
&\leq \frac{1}{2^{N/2}}
\end{aligned}$$

where we have used $\sum_{z\in\mathcal{E}_t}E^t_z \leq \mathbf{1}_B$ and $\sum_{x\in\mathcal{F}_s}F^s_x \leq \mathbf{1}_E$. As $|\{t|l(t) \leq l\}| \leq 2^{l+1}$ and $|\{s|l(s) \leq m\}| \leq 2^{m+1}$ hold, we obtain

$$\mathrm{tr}(\Theta\hat{P}_l) + \mathrm{tr}(\Theta\hat{Q}_m) \leq 1 + 2^{\frac{l+m-N+3}{2}}$$

This inequality with (1) and (2) derives

$$\left|\{z|K_{c,U}(z|\rho^B_z, Z) \leq l\}\right| + \left|\{x|K_{c,U}(x|\sigma^E_x, X) \leq m\}\right| \leq 2^N\left(1 + 2^{\frac{l+m-N+3}{2}}\right)$$

Taking into consideration the relationship between $K_{c,U}$ and K_U, we finally obtain

$$\left|\{z|K(z|\rho^B_z, Z) \leq l\}\right| + \left|\{x|K(x|\sigma^E_x, X) \leq m\}\right| \leq 2^N\left(1 + 2^{\frac{l+m-N}{2}+c}\right)$$

where c is a constant. Q.E.D.

Let us consider the implication of the above theorem. As noted in the theorem, a nontrivial bound is given only for $l + m \leq N - 2c$. This situation is attained when one considers the asymptotic behavior of a family of protocols governed by increasing N. We consider $\{z|K(z|\rho^B_z, Z) \leq p_ZN\}$ and $\{x|K(x|\sigma^E_x, X) \leq p_xN\}$ for some $p_Z, p_X \in [0,1]$. If p_Z and p_X satisfy $p_Z + p_X < 1$, for a sufficiently large $N > 0$, the right-hand side of the above theorem behaves as $2^N(1+O(2^{-\epsilon N}))$ for some $\epsilon > 0$. That is, for any $p_Z, p_X \in [0,1)$ satisfying $p_X + p_Z < 1$, there exists $\epsilon > 0$ such that it holds

$$|\{z|K(z|\rho^B_z, Z) \leq p_ZN\}| + |\{x|K(x|\sigma^E_x, X) \leq p_XN\}| \leq 2^N(1 + O(2^{-\epsilon N}))$$

This type of argument is common in the algorithmic information theory.

In addition, the above theorem gives the following corollaries, which should be meaningful for an asymptotically large N.

Corollary 1 *There exists a trade-off relationship between* $\max_z K(z|\rho_z^B, Z)$ *and* $\max_x K(x|\sigma_x^E, X)$*:*

$$\max_{z\in\{0,1\}^N} K(z|\rho_z^B, Z) + \max_{x\in\{0,1\}^N} K(x|\sigma_x^E, X) \geq N - O(1)$$

Proof: Because for $l = \max_z K(z|\rho_z^B, Z)$ and $m = \max_x K(x|\sigma_x^E, X)$, $\{z|K(z|\rho_z^B, Z) \leq l\}| = 2^N$ and $\{x|K(x|\sigma_x^E, X) \leq m\}| = 2^N$ hold, the right-hand side of the above theorem must be larger than $2^N(1+1)$. It is only possible when $l + m \geq N - 2c$ holds. Q.E.D.

Corollary 2 *(No-cloning theorem [31,32]) Unknown states cannot be cloned (for a sufficiently large N).*

Proof: Suppose that universal cloning is possible. Put $\mathcal{H}_B \simeq \mathcal{H}_E \simeq \mathcal{H}_A$. There should exist a CP-map Λ satisfying both $\Lambda(|z\rangle\langle z|) = |z\rangle\langle z| \otimes |z\rangle\langle z|$ and $\Lambda(|\overline{x}\rangle\langle\overline{x}|) = |\overline{x}\rangle\langle\overline{x}| \otimes |\overline{x}\rangle\langle\overline{x}|$ for all $z, x \in \{0,1\}^N$. It implies that $\max_z K(z|\rho_z^B, Z) = O(1)$ and $\max_x K(x|\sigma_x^E, X) = O(1)$. This contradicts corollary 1. Q.E.D.

4. Discussion

In this research, we study a quantum algorithmic information-theoretic representation of the information-disturbance theorem. We first discuss the relationship between Shannon's information-theoretic theorem and our algorithmic one. Using a possible relationship between Shannon information and Kolmogorov complexity is likely to yield an inequality

$$\sum_{z\in\{0,1\}^N} p_Z(z)K(z|\rho_z^B, Z) + \sum_{x\in\{0,1\}^N} p_X(x)K(x|\sigma_x^E, X) \geq N - c \tag{3}$$

directly from Shannon's version. This inequality is different from our theorem derived in the present paper. In fact, even if families $\{K(z|\rho_z^B, Z)\}_z$ and $\{K(x|\sigma_x^E, X)\}_x$ satisfy this inequality, they may not satisfy the inequality in our theorem. In fact, if we put $|\{z|K(z|\rho_z^B, Z) = \frac{N}{2}\}| = \frac{3\cdot 2^N}{4}$, $|\{z|K(z|\rho_z^B, Z) = N\}| = \frac{2^N}{4}$, $|\{x|K(x|\sigma_x^E, X) = \frac{N}{3}\}| = \frac{3\cdot 2^N}{4}$, and $|\{x|K(x|\sigma_x^E, X) = N\}| = \frac{2^N}{4}$, then the left-hand side of (3) becomes $\frac{9N}{8}$, but our theorem (with $c = 0$) is not satisfied for $l = \frac{N}{2}$ and $m = \frac{N}{3}$. It would be interesting to investigate an inequality for Shannon's information that corresponds to our theorem.

As mentioned in the introduction, one of the purposes of this study is to demonstrate the usage of quantum Kolmogorov complexity in the quantum information theory. Our derivation dealt with Kolmogorov complexity directly without relying on the results known in Shannon's version of the quantum information theory. Those results imply that Kolmogorov complexity can yield meaningful results by combining it with the uncertainty relation. Thus, quantum Kolmogorov complexity by itself can be a powerful tool in the quantum information theory by itself.

In addition, as mentioned earlier, there are various quantum versions of Kolmogorov complexity. It would be interesting and important to study quantum information-theoretic problems by using these quantum versions.

While our information-disturbance theorem was formulated in a cryptographic setting, it is strongly related to Heisenberg's uncertainty principle, which is one of the most important characteristics of quantum mechanics. According to Heisenberg's original Gedanken experiment, a precise measurement of the momentum destroys the position of a particle. If one regards Eve's attack as the measurement of "momentum", the information-disturbance relationship that predicts a disturbance in the conjugate "position" corresponds to the Heisenberg's setting. However, despite this similarity, there is a gap between our information-disturbance theorem and Heisenberg's uncertainty principle. The latter should be formulated as a relationship that does not depend on states as was discussed in [33]. Further investigation in this direction needs to be carried out. Besides exploring subjects related to the uncertainty principle, several things need to be done. We hope that the quantum Kolmogorov complexity will shed new light on the quantum information theory.

Acknowledgments

I would like to thank K. Imafuku and anonymous referees for valuable discussions and comments.

References and Notes

1. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509.
2. Grover, L.K. A fast quantum mechanical algorithm for database search. In Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; p. 212.
3. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India, 10–12 December 1984; p. 175.
4. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663.
5. Kolmogorov, A.N. Three approaches to the quantitative definition of information. *Probl. Inform. Transm.* **1965**, *1*, 1–7.
6. Chaitin, G.J. On the length of programs for computing finite binary sequences: Statistical considerations. *J. Assoc. Comput. Mach.* **1969**, *16*, 145.
7. Li, M.; Vitányi, P.M.B. *An Introduction to Kolmogorov Complexity and Its Applications*. Springer-Verlag: New York, NY, USA, 1997.
8. Vitányi, P.M.B. Quantum kolmogorov complexity based on classical descriptions. *IEEE Trans. Inform. Theory* **2001**, *47*, 2464.
9. Svozil, K. Quantum algorithmic information theory. *J. Univers. Comput. Sci.* **1996**, *2*, 311.
10. Berthiaume, A.; van Dam, W.; Laplante, S. Quantum Kolmogorov complexity. *J. Comput. System. Sci.* **2001**, *63*, 201.
11. Gacs, P. Quantum algorithmic entropy. *J. Phys. A: Math. Gen.* **2001**, *34*, 1.
12. Mora, C; Briegel, H; Kraus, B, Quantum Kolmogorov complexity and its applications. *Int. J. Quantum Inform.* **2006**, *5*, 12.
13. Benatti, F; Krüger, T; Müller, M; Siegmund-Schultze, R; Szkora, A. Entropy and quantum Kolmogorov complexity: A quantum Brudno's theorem. *Commun. Math. Phys.* **2006**, *265*, 437.
14. Miyadera, T.; Imai, H. Quantum Kolmogorov complexity and quantum key distribution. *Phys. Rev. A* **2009**, *79*, 012324.

15. Boykin, P.O.; Roychowdhuri, V.P. Information *vs.* Disturbance in Dimension D. *Quantum Inf. Comput.* **2005**, *5*, 396.
16. Miyadera, T.; Imai, H. Information-disturbance theorem for mutually unbiased observables. *Phys. Rev. A* **2006**, *73*, 042317.
17. Miyadera, T.; Imai, H. Information-disturbance theorem and uncertainty relation. *arXiv* **2007**, arXiv:0707.4559.
18. Biham, E.; Boyer, M.; Boykin, P.O.; Mor, T.; Roychowdhury, V.P. A proof of the security of quantum key distribution. *J. Cryptology* **2006**, *19*, 381.
19. Deutsch, D. Quantum theory, the church-turing principle and the universal quantum computer. *Proc. Roy. Soc. Lond. A* **1985**, *400*, 96.
20. Bernstein, A.; Vazirani, U. Quantum complexity theory. *SIAM J. Comput.* **1997**, *26*, 1411.
21. Müller, M. Strongly universal quantum turing machines and invariance of Kolmogorov complexity. *IEEE Trans. Inform. Theory* **2008**, *54*, 763.
22. Müller, M. Quantum Kolmogorov complexity and the quantum turing machine. Ph.D. Thesis, Technical University of Berlin, Berlin, Germany, 2007; arXiv:0712.4377.
23. Myers, J.M. Can a universal quantum computer be fully quantum? *Phys. Rev. Lett.* **1997**, *78*, 1823.
24. Linden, N.; Popescu, S. The halting problem for quantum computers. *arXiv* **1998**, arXiv:quant-ph/9806054.
25. Ozawa, M. Quantum nondemolition monitoring of universal quantum computers. *Phys. Rev. Lett.* **1998**, *80*, 631.
26. Miyadera, T.; Ohya, M. On halting process of quantum Turing machine. *Open Sys. Info. Dyn.* **2005**, *12*, 261.
27. The word "probabilistically" here is used to mean "randomly in a probabilistic sense". That is, we use an unbiased probability $1/|\Omega|$ to choose a sample from a sample space Ω (say $\Omega = \{0,1\}^{2N}$). (To avoid a possible confusion of it with randomness in algorithmic sense, we just write "probabilistically".)
28. To treat ρ_z^B and σ_x^E as an auxiliary input for a quantum Turing machine, they have to be somehow represented as states on a system consisting of qubits. Our discussion does not depend on how we identify them.
29. In general, *a posteriori* state after a measurement is determined as follows. Suppose that there exist two system A and B that are described by Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. Let us consider a state ρ over the bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$. Suppose that on A one made a measurement described by a positive-operator-valued measure (POVM) $F = \{F_x\}$ and obtained an outcome x. *A posteriori* state on the system B conditioned with this x becomes

$$\rho_x = \frac{\mathrm{tr}_A(\rho(F_x \otimes \mathbf{1}))}{\mathrm{tr}\rho F_x \otimes \mathbf{1})}$$

That is, it is a unique state that satisfies $\mathrm{tr}(\rho_x G)\mathrm{tr}(\rho(F_x \otimes \mathbf{1})) = \mathrm{tr}(\rho(F_x \otimes G))$ for any operator G on $\mathcal{H}_B$.
30. Miyadera, T.; Imai, H. Generalized Landau-Pollak uncertainty relation. *Phys. Rev. A* **2007**, *76*, 062108.

31. Wootters, W.K.; Zurek, W. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802.
32. Miyadera,T; Imai, H. No-cloning theorem on quantum logics. *J. Math. Phys.* **2009**, *50*, 102107.
33. Miyadera, T.; Imai, H. Heisenberg's uncertainty principle for simultaneous measurement of positive-operator-valued measures. *Phys. Rev. A* **2008**, *78*, 052119.