情報力学とその応用
―複雑系から量子コンピュータまで―

東京理科大学理工学部情報科学科
大矢雅則

要旨

物理学，数学，工学，生物学，経済学などで扱われている”系（システム）”の”力学”は，系を記述する状態の変化を調べることよってなされている．系の大きさがある程度以上になると，その系を構成している 個々の元の特質の単なる線形的な重ね合わせでは系全体の示す特徴的な力学を記述することができなくなる．こうした系を複雑系といい，現在様々な研究がなされているが，第一原理から出発した統一的な研究は少ない．この統一的研究への試みの一つが情報力学である．情報力学では，複雑系の力学を調べるために，様々な分野で個別に扱われていた系の複雑さと状態変化の力学とを融合して，新たな二つの複雑量を導入する．これらの複雑量をベースにして，状態変化を与える力学のカオス性や状態そのものの複雑度を測る尺度を定め，力学系の分類に役立てる．

本稿では，情報力学のスキームにおいて，ここ数年私の研究室で行われてきた研究のいくつかを紹介する．主に，以下の話題にふれる．

[1]．近年，光通信，光メモリー，量子コンピュータなどの新たな技術が将来の情報処理において重要な役割を果たすと期待されている．これらはいずれも，大容量な情報をより速く確実にアクセスするための技術である．近い将来，実現されることが期待されているこうした技術の布石となる理論を目指した基礎的研究が，量子情報理論である．この量子情報理論の数学的基礎，及びその一部である量子コンピュータ基礎理論である量子エンタグルド状態の分類，量子テレポーテーションなどの話題を解説する．

[2]．量子系カオスを記述する尺度をどのように作るか．また，それを具体的に計算するアルゴリズムは可能かについて述べる．

[3]．最近（Dec.1999），私とモスクワのVolovich氏とで，２０年来の懸案であった”ＮＰ完全問題が多項式 時間で解けるか”という問題を肯定的に解くことに成功したが，この計算複雑量の問題にも簡単に触れる．

[4]．その他の話題として，生命の情報を伝搬するゲノムの構造とその変化は情報力学的にどう扱われるかを，解説する．

Part I
Quantum Information

1 Quantum Mutual Entropy

The quantum mutual entropy was introduced in [52] for a quantum input and quantum output, namely, for purely quantum channel, and it was generalized for a general quantum system described by C*-algebraic terminology[54]. We here review the quantum mutual entropy in usual quantum system described by a Hilbert space.

Let $\mathcal{H}$ be a Hilbert space for an input space, $B(\mathcal{H})$ be the set of all bounded linear operators on $\mathcal{H}$ and $\mathcal{S}(\mathcal{H})$ be the set of all density operators on $\mathcal{H}$. An output space is described by another Hilbert space $\tilde{\mathcal{H}}$, but often $\mathcal{H} = \tilde{\mathcal{H}}$. A channel from the input system to the output system is a mapping Λ^* from $\mathcal{S}(\mathcal{H})$ to $\mathcal{S}(\tilde{\mathcal{H}})$ [51]. A channel Λ^* is said to be completely positive if the dual map Λ satisfies the following condition: $\Sigma_{k,j=1}^{n} A_k^* \Lambda(B_k^* B_j) A_j \geq 0$ for any $n \in \mathbf{N}$ and any $A_j \in B(\mathcal{H}), B_j \in B(\tilde{\mathcal{H}})$.

An input state $\rho \in \mathcal{S}(\mathcal{H})$ is sent to the output system through a channel Λ^*, so that the output state is written as $\tilde{\rho} \equiv \Lambda^* \rho$. Then it is important to ask how much information of ρ is correctly sent to the output state $\Lambda^* \rho$. This amount of information transmitted from input to output is expressed by the mutual entropy in Shannon's theory.

In order to define the quantum mutual entropy, we first mention the entropy of a quantum state introduced by von Neumann[50]. For a state ρ, there exists a unique spectral decomposition

$$\rho = \Sigma_k \lambda_k P_k, \tag{1.1}$$

where λ_k is an eigenvalue of ρ and P_k is the associated projection for each λ_k. The projection P_k is not one-dimensional when λ_k is degenerated, so that the spectral decomposition can be further decomposed into one-dimensional projections. Such a decomposition is called a Schatten decomposition, namely,

$$\rho = \Sigma_k \lambda_k E_k, \tag{1.2}$$

where E_k is the one-dimensional projection associated with λ_k and the degenerated eigenvalue λ_k repeats $\dim P_k$ times. This Schatten decomposition

is not unique unless every eigenvalue is non-degenerated. Then the entropy (von Neumann entropy) $S(\rho)$ of a state ρ is defined by

$$S(\rho) = -tr\rho\log\rho, \tag{1.3}$$

which equals to the Shannon entropy of the probability distribution $\{\lambda_k\}$:

$$S(\rho) = -\sum_k \lambda_k \log\lambda_k. \tag{1.4}$$

The quantum mutual entropy was introduced on the basis of the above von Neumann entropy for purely quantum communication processes. The mutual entropy depends on an input state ρ and a channel Λ^*, so it is denoted by $I(\rho;\Lambda^*)$, which should satisfy the following conditions:

(1) The quantum mutual entropy is well-matched to the von Neumann entropy. Furthermore, if a channel is trivial, i.e., Λ^* = identity map, then the mutual entropy equals to the von Neumann entropy: $I(\rho;id) = S(\rho)$.

(2) When the system is classical, the quantum mutual entropy reduces to classical one.

(3) Shannon's fundamental inequality $0 \leq I(\rho;\Lambda^*) \leq S(\rho)$ is held.

Before mentioning the quantum mutual entropy, we briefly review the classical mutual entropy. Let $(\Omega,\mathcal{F})$, $(\overline{\Omega},\overline{\mathcal{F}})$be an input and output measurable spaces, respectively, and $P(\Omega)$, $P(\overline{\Omega})$ are the corresponding set of all probability measures (states). A channel Λ^* is a mapping from $P(\Omega)$ to $P(\overline{\Omega})$ and its dual Λ is a map from the set $B(\Omega)$ of all Baire measurable functions on Ω to $B(\overline{\Omega})$. For an input state $\mu \in P(\Omega)$, the output state $\overline{\mu} = \Lambda^*\mu$ and the joint state (probability measure) Φ is given by

$$\Phi(Q \times \overline{Q}) = \int_{\overline{Q}} \Lambda(1_Q)\, d\mu,\ Q \in \mathcal{F},\ \overline{Q} \in \overline{\mathcal{F}}, \tag{1.5}$$

where 1_Q is the characteristic function on Ω : $1_Q(\omega) = \begin{cases} 1 & (\omega \in Q) \\ 0 & (\omega \notin Q) \end{cases}$. The classical entropy, relative entropy and mutual entropy are defined as follows:

$$S(\mu) = \sup\left\{-\sum_{k=1}^{n} \mu(A_k)\log\mu(A_k);\{A_k\} \in \mathcal{P}(\Omega)\right\}, \tag{1.6}$$

$$S(\mu,\nu) = \sup\left\{\sum_{k=1}^{n} \mu(A_k)\log\frac{\mu(A_k)}{\nu(A_k)};\{A_k\} \in \mathcal{P}(\Omega)\right\}, \tag{1.7}$$

$$I(\mu;\Lambda^*) = S(\Phi, \mu \otimes \Lambda^*\mu), \tag{1.8}$$

where $\mathcal{P}(\Omega)$ is the set of all finite partitions on Ω, that is, $\{A_k\} \in \mathcal{P}(\Omega)$ iff $A_k \in \mathcal{F}$ with $A_k \cap A_j = \emptyset$ $(k \neq j)$and $\cup_{k=1}^{n} A_k = \Omega$.

In order to define the quantum mutual entropy, we need the joint state (it is called "compound state" in the sequel) describing the correlation between an input state ρ and the output state $\Lambda^*\rho$ and the quantum relative entropy. A finite partition of Ω in classical case corresponds to an orthogonal decomposition $\{E_k\}$ of the identity operator I of $\mathcal{H}$ in quantum case because the set of all orthogonal projections is considered to make an event system for a quantum system. It is known [70]that the following equality holds

$$\sup\left\{-\sum_k tr\rho E_k \log tr\rho E_k; \{E_k\}\right\} = -tr\rho\log\rho,$$

and the supremum is attained when $\{E_k\}$ is composed of the Schatten decomposition of ρ. Therefore the Schatten decomposition is used to define the compound state and the quantum mutual entropy.

The compound state θ_E (corresponding to joint state in CS) of ρ and $\Lambda^*\rho$ was introduced in [52, 53], which is given by

$$\theta_E = \sum_k \lambda_k E_k \otimes \Lambda^* E_k, \tag{1.9}$$

where E stands for a Schatten decomposition of ρ, so that the compound state depends on how we decompose the state ρ into basic states (elementary events), in other words, how to see the input state.

The relative entropy for two states ρ and σ is defined by Umegaki [86] and Lindblad [42], which is written as

$$S(\rho,\sigma) = \begin{cases} tr\rho(\log\rho - \log\sigma) & (\text{when } \overline{ran\rho} \subset \overline{ran\sigma}) \\ \infty & (\text{otherwise}) \end{cases} \tag{1.10}$$

Then we can define the mutual entropy by means of the compound state and the relative entropy [52], that is,

$$I(\rho;\Lambda^*) = \sup\{S(\theta_E, \rho\otimes\Lambda^*\rho); E = \{E_k\}\}, \tag{1.11}$$

where the supremum is taken over all Schatten decompositions. Some computations reduce it to the following form:

$$I(\rho;\Lambda^*)=\sup\left\{\sum_k \lambda_k S(\Lambda^* E_k,\Lambda^*\rho)\,;E=\{E_k\}\right\}, \tag{1.12}$$

This mutual entropy satisfies all conditions (1)$\sim$(3) mentioned above.

When the input system is classical, an input state ρ is given by a probability distribution or a probability measure, in either case, the Schatten decomposition of ρ is unique, namely, for the case of probability distribution ; $\rho=\{\lambda_k\}$,

$$\rho=\sum_k \lambda_k \delta_k, \tag{1.13}$$

where δ_k is the delta measure, that is,

$$\delta_k(j)=\delta_{k,j}=\begin{cases}1(k=j)\\0(k\neq j)\end{cases},\forall j. \tag{1.14}$$

Therefore for any channel Λ^*, the mutual entropy becomes

$$I(\rho;\Lambda^*)=\sum_k \lambda_k S(\Lambda^*\delta_k,\Lambda^*\rho), \tag{1.15}$$

which equals to the following usual expression of Shannon when it is well-defined:

$$I(\rho;\Lambda^*)=S(\Lambda^*\rho)-\sum_k \lambda_k S(\Lambda^*\delta_k), \tag{1.16}$$

which has been taken as the definition of the mutual entropy for a classical-quantum(-classical) channel [9, 14, 28, 30, 41].

Note that the above definition of the mutual entropy (1.12) is written as

$$\begin{aligned} & I(\rho;\Lambda^*)\\ =\ & \sup\left\{\sum_k \lambda_k S(\Lambda^*\rho_k,\Lambda^*\rho)\,;\rho=\sum_k \lambda_k\rho_k\in F_o(\rho)\right\}, \end{aligned}$$

where $F_o(\rho)$ is the set of all orthogonal finite decompositions of ρ [63].

More general formulation of the mutual entropy for general quantum systems was done [54, 31] in C*dynamical system by using Araki's or Uhlmann's relative entropy[7, 85, 70]. This general mutual entropy contains all other cases including measure theoretic definition of Gelfand and Yaglom [25].

2 Communication Processes

The information communication process is mathematically set as follows: M messages are sent to a receiver and the kth message $\omega^{(k)}$ occurs with the probability λ_k. Then the occurrence probability of each message in the sequence $\left(\omega^{(1)}, \omega^{(2)}, \cdots, \omega^{(M)}\right)$of M messages is denoted by $\rho = \{\lambda_k\}$, which is a state in a classical system. If ξ is a classical coding, then $\xi(\omega)$ is a classical object such as an electric pulse. If ξ is a quantum coding, then $\xi(\omega)$ is a quantum object (state) such as a coherent state. Here we consider such a quantum coding, that is, $\xi\left(\omega^{(k)}\right)$ is a quantum state, and we denote $\xi\left(\omega^{(k)}\right)$ by σ_k. Thus the coded state for the sequence $\left(\omega^{(1)}, \omega^{(2)}, \cdots, \omega^{(M)}\right)$ is written as

$$\sigma = \sum_k \lambda_k \sigma_k. \tag{2.1}$$

This state is transmitted through a channel γ, which is expressed by a completely positive mapping Γ^* from the state space of X to that of $\widetilde{X}$, hence the output coded quantum state $\widetilde{\sigma}$ is $\Gamma^*\sigma$. Since the information transmission process can be understood as a process of state (probability) change, when Ω and $\widetilde{\Omega}$ are classical and X and $\widetilde{X}$ are quantum, the whole transmission process is written as

$$P(\Omega) \xrightarrow{\Xi^*} \mathcal{S}(\mathcal{H}) \xrightarrow{\Gamma^*} \mathcal{S}(\widetilde{\mathcal{H}}) \xrightarrow{\widetilde{\Xi}^*} P(\widetilde{\Omega}), \tag{2.2}$$

where Ξ^* (resp.$\widetilde{\Xi}^*$) is the channel corresponding to the coding ξ (resp.$\widetilde{\xi}$) and $\mathcal{S}(\mathcal{H})$ (resp.$\mathcal{S}(\widetilde{\mathcal{H}})$) is the set of all density operators (states) on $\mathcal{H}$ (resp.$\widetilde{\mathcal{H}}$).

We have to be care to study the objects in the above transmission process (2.2). Namely, we have to make clear which object is going to study. For instance, if we want to know the information capacity of a quantum channel $\gamma(=\Gamma^*)$, then we have to take X so as to describe a quantum system like

a Hilbert space and we need to start the study from a quantum state in quantum space X not from a classical state associated to a message. If we like to know the capacity of the whole process including a coding and a decoding, which means the capacity of a channel $\tilde{\xi} \circ \gamma \circ \xi (= \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*)$, then we have to start from a classical state. In any case, when we concern the capacity of channel, we have only to take the supremum of the mutual entropy $I(\rho; \Lambda^*)$ over a quantum or classical state ρ in a proper set determined by what we like to study with a channel Λ^*. We explain this more precisely in the next section.

3 Channel Capacity

We discuss two types of channel capacity in communication processes, namely, the capacity of a quantum channel Γ^* and that of a classical (classical-quantum-classical) channel $\tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*$.

(1) *Capacity of quantum channel:* The capacity of a quantum channel is the ability of information transmission of a quantum channel itself, so that it does not depend on how to code a message being treated as classical object and we have to start from an arbitrary quantum state and find the supremum of the quantum mutual entropy. One often makes a mistake in this point. For example, one starts from the coding of a message and compute the supremum of the mutual entropy and he says that the supremum is the capacity of a quantum channel, which is not correct. Even when his coding is a quantum coding and he sends the coded message to a receiver through a quantum channel, if he starts from a classical state, then his capacity is not the capacity of the quantum channel itself. In his case, usual Shannon's theory is applied because he can easily compute the conditional distribution by a usual (classical) way. His supremum is the capacity of a classical-quantum-classical channel, and it is in the second category discussed below.

The capacity of a quantum channel Γ^* is defined as follows: Let $\mathcal{S}_0 (\subset \mathcal{S}(\mathcal{H}))$ be the set of all states prepared for expression of information. Then the capacity of the channel Γ^* with respect to $\mathcal{S}_0$ is defined by

$$C^{\mathcal{S}_0}(\Gamma^*) = \sup\{I(\rho; \Gamma^*) ; \rho \in \mathcal{S}_0\}. \tag{3.1}$$

Here $I(\rho; \Gamma^*)$ is the mutual entropy given in (1.11) or (1.12) with $\Lambda^* = \Gamma^*$. When $\mathcal{S}_0 = \mathcal{S}(\mathcal{H})$, $C^{\mathcal{S}(\mathcal{H})}(\Gamma^*)$ is denoted by $C(\Gamma^*)$ for simplicity. The

capacity $C(\Gamma^*)$ is written as

$$C(\Gamma^*) = \sup\{I(\rho;\Gamma^*)\,;\rho\in\mathcal{S}(\mathcal{H})\}, \tag{3.2}$$

where the supremum is taken over all states ρ with its orthogonal pure decomposition $\sum_k \lambda_k\rho_k$ of ρ. In [71, 48], we also considered the pseudo-quantum capacity $C_p(\Gamma^*)$ defined by (3.1) with the pseudo-mutual entropy $I_p(\rho;\Gamma^*)$ where the supremum is taken over all finite decompositions instead of all orthogonal pure decompositions:

$$\begin{aligned} I_p(\rho;\Gamma^*) \;=\; \sup\Bigg\{&\sum_k \lambda_k S(\Gamma^*\rho_k,\Gamma^*\rho)\,;\rho=\sum_k\lambda_k\rho_k,\\ &\text{finite decomposition}\Bigg\}. \end{aligned} \tag{3.3}$$

However the pseudo-mutual entropy is not well-matched to the conditions explained in Sec.1, and it is difficult to be computed numerically. The relation between $C(\Gamma^*)$ and $C_p(\Gamma^*)$ was discussed in[71]. From the monotonicity of the mutual entropy[70], we have

$$0\le C^{\mathcal{S}_0}(\Gamma^*)\le C_p^{\mathcal{S}_0}(\Gamma^*)\le\sup\{S(\rho);\rho\in\mathcal{S}_0\}.$$

(2) *Capacity of classical-quantum-classical channel:* The capacity of C-Q-C channel $\tilde{\Xi}^*\circ\Gamma^*\circ\Xi^*$ is the capacity of the information transmission process starting from the coding of messages, therefore it can be considered as the capacity including a coding (and a decoding). As is discussed in Sec.2, an input state ρ is the probability distribution $\{\lambda_k\}$ of messages, and its Schatten decomposition is unique as (1.13), so the mutual entropy is written by (1.15):

$$\begin{aligned} &I\left(\rho;\tilde{\Xi}^*\circ\Gamma^*\circ\Xi^*\right)\\ =\;&\sum_k\lambda_k S\left(\tilde{\Xi}^*\circ\Gamma^*\circ\Xi^*\delta_k,\tilde{\Xi}^*\circ\Gamma^*\circ\Xi^*\rho\right). \end{aligned} \tag{3.4}$$

If the coding Ξ^* is a quantum coding, then $\Xi^*\delta_k$ is expressed by a quantum state. Let denote the coded quantum state by σ_k and put $\sigma=\Xi^*\rho=\sum_k\lambda_k\sigma_k$. Then the above mutual entropy is written as

$$I\left(\rho;\tilde{\Xi}^*\circ\Gamma^*\circ\Xi^*\right)=\sum_k\lambda_k S\left(\tilde{\Xi}^*\circ\Gamma^*\sigma_k,\tilde{\Xi}^*\circ\Gamma^*\sigma\right). \tag{3.5}$$

This is the expression of the mutual entropy of the whole information transmission process starting from a coding of classical messages. Hence the capacity of C-Q-C channel is

$$C^{P_0}\left(\tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*\right) = \sup\{I\left(\rho; \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*\right); \rho \in P_0\}, \tag{3.6}$$

where $P_0 (\subset P(\Omega))$ is the set of all probability distributions prepared for input (a-priori) states (distributions or probability measures). Moreover the capacity for coding free is found by taking the supremum of the mutual entropy (3.4) over all probability distributions and all codings Ξ^*:

$$C_c^{P_0}\left(\tilde{\Xi}^* \circ \Gamma^*\right) = \sup\{I\left(\rho; \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*\right); \rho \in P_0, \Xi^*\}. \tag{3.7}$$

The last capacity is for both coding and decoding free and it is given by

$$C_{cd}^{P_0}(\Gamma^*) = \sup\{I\left(\rho; \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*\right); \rho \in P_0, \Xi^*, \tilde{\Xi}^*\}. \tag{3.8}$$

These capacities $C_c^{P_0}$, $C_{cd}^{P_0}$ do not measure the ability of the quantum channel Γ^* itself, but measure the ability of Γ^* through the coding and decoding.

Remark that $\sum_k \lambda_k S(\Gamma^* \sigma_k)$ is finite, then (3.4) becomes

$$I\left(\rho; \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*\right) = S(\tilde{\Xi}^* \circ \Gamma^* \sigma) - \sum_k \lambda_k S(\tilde{\Xi}^* \circ \Gamma^* \sigma_k). \tag{3.9}$$

Further, if ρ is a probability measure having a density function $f(\lambda)$ and each λ corresponds to a quantum coded state $\sigma(\lambda)$, then $\sigma = \int f(\lambda)\, \sigma(\lambda) d\lambda$ and

$$\begin{aligned} & I\left(\rho; \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*\right) \\ = \; & S(\tilde{\Xi}^* \circ \Gamma^* \sigma) - \int f(\lambda) S(\tilde{\Xi}^* \circ \Gamma^* \sigma(\lambda)) d\lambda. \end{aligned} \tag{3.10}$$

This is bounded by

$$S(\Gamma^* \sigma) - \int f(\lambda) S(\Gamma^* \sigma(\lambda)) d\lambda,$$

which is called the Holevo bound and is computed in several occasions [89, 71]

The above three capacities C^{P_0}, $C_c^{P_0}$, $C_{cd}^{P_0}$ satisfy the following inequalities

$$\begin{aligned} 0 \; & \leq \; C^{P_0}\left(\tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*\right) \leq C_c^{P_0}\left(\tilde{\Xi}^* \circ \Gamma^*\right) \\ & \leq \; C_{cd}^{P_0}(\Gamma^*) \leq \sup\{S(\rho); \rho \in P_o\} \end{aligned}$$

where $S(\rho)$ is not the von Neumann entropy but the Shannon entropy: $-\sum \lambda_k \log \lambda_k$.

The capacities (3.1), (3.6),(3.7) and (3.8) are generally different. Some misunderstandings occur due to forgetting which channel is considered. That is, we have to make clear what kind of the ability (capacity) is considered, the capacity of a quantum channel itself or that of a classical-quantum(-classical) channel. The computation of the capacity of a quantum channel was carried in several models in [71, 72]

4 Quantum Entanglements

Recently the quantum entangled state has been mathematically studied [11, 43, 76], in which the entangled state is defined by a state not written as a form $\sum_k \lambda_k \rho_k \otimes \sigma_k$ with any states ρ_k and σ_k. A state written as above is called a separable state, so that an entangled state is a state not belonged to the set of all separable states. However it is obvious that there exist several correlated states written as separable forms. Such correlated states have been discussed in several contexts in quantum probability such as quantum filtering [9], quantum compound state [52], quantum Markov state [1] and quantum lifting [2]. In [13], we showed a mathematical construction of quantum entangled states and gave a finer classification of quantum sates.

For the (separable) Hilbert space $\mathcal{K}$ of a quantum system, let $\mathcal{A} \equiv B(\mathcal{K})$ be the set of all linear bounded operators on $\mathcal{K}$. A normal state φ on $\mathcal{A}$ can be expressed as $\varphi(A) = tr_{\mathcal{G}} \kappa^\dagger A \kappa$, $A \in \mathcal{A}$, where $\mathcal{G}$ is another separable Hilbert space, κ is a linear Hilbert-Schmidt operator from $\mathcal{G}$ to $\mathcal{K}$ and $\kappa^\dagger$ is the adjoint operator of κ from $\mathcal{K}$ to $\mathcal{G}$. The (unique) density operator $\sigma \in \mathcal{A}$ associated to the state $\varphi : \varphi(A) = tr A\sigma$, $A \in \mathcal{A}$, is written by κ such as $\sigma = \kappa\kappa^\dagger$. This κ is called the amplitude operator, and it is called just the amplitude if $\mathcal{G}$ is one dimensional space $\mathbb{C}$, corresponding to the pure state $\varphi(A) = \kappa^\dagger A \kappa$ for a $\kappa \in \mathcal{K}$ with $\kappa^\dagger \kappa = \|\kappa\|^2 = 1$. In general, $\mathcal{G}$ is not one dimensional, the dimensionality $\dim \mathcal{G}$ must be not less than $\dim \sigma\mathcal{K}$.

Since $\mathcal{G}$ is separable, $\mathcal{G}$ is realized as a subspace of $l^2(\mathbf{N})$ of complex sequences ($i.e., \zeta^\bullet = (\zeta^n)$, $\zeta^n \in \mathbb{C}$, $n \in \mathbf{N}$ with $\sum |\zeta^n|^2 < +\infty$), so that any vector $\zeta^\bullet = (\zeta^n)$ represents a vector $\zeta = \sum \zeta^n |n\rangle$ in the standard basis $\{|n\rangle\} \in \mathcal{G}$ of $l^2(\mathbf{N})$.

Given the amplitude operator κ, one can define not only the states $\sigma \equiv \kappa\kappa^\dagger$ and $\rho \equiv \kappa^\dagger\kappa$ on the algebras $\mathcal{A}(= B(\mathcal{K}))$ and $\mathcal{B}(= B(\mathcal{G}))$ but also an

entanglement state Θ on the algebra $\mathcal{B} \otimes \mathcal{A}$ of all bounded operators on the tensor product Hilbert space $\mathcal{G} \otimes \mathcal{K}$ by

$$\Theta(B \otimes A) = tr_{\mathcal{G}} B\kappa^{\dagger} A\kappa = tr_{\mathcal{K}} A\kappa B\kappa^{\dagger}$$

for any $B \in \mathcal{B}$. This state is pure as it is the case of $\mathcal{F} = \mathbb{C}$ in the theorem below, and it satisfies the marginal conditions: For any $B \in \mathcal{B}, A \in \mathcal{A}$,

$$\Theta(B \otimes I) = tr_{\mathcal{G}} B\rho, \quad \Theta(I \otimes A) = tr_{\mathcal{K}} A\sigma.$$

Theorem 4.1 *[13]Let $\Theta : \mathcal{B} \otimes \mathcal{A} \to \mathbb{C}$ be a state*

$$\Theta(B \otimes A) = tr_{\mathcal{F}} \psi^{\dagger}(B \otimes A)\psi, \tag{4.1}$$

defined by an amplitude operator ψ on a separable Hilbert space $\mathcal{E}$ into the tensor product Hilbert space $\mathcal{G} \otimes \mathcal{K}$; $\psi : \mathcal{E} \to \mathcal{G} \otimes \mathcal{K}$ with $tr_{\mathcal{F}} \psi^{\dagger}\psi = 1$. Then there exists an amplitude operator $\kappa : \mathcal{G} \to \mathcal{F} \otimes \mathcal{K}$ such that the state Θ can be achieved by an entanglement

$$\Theta(B \otimes A) = tr_{\mathcal{G}} B\kappa^{\dagger}(I \otimes A)\kappa = tr_{\mathcal{F}\otimes\mathcal{K}}(I \otimes A)\kappa B\kappa^{\dagger} \tag{4.2}$$

The entangling operator κ is uniquely defined up to a unitary transformation of the minimal space $\mathcal{F}$.

The entangled state (4.2) is written as

$$\Theta(B \otimes A) = tr_{\mathcal{G}} B\phi(A) = tr_{\mathcal{K}} A\phi_*(B), \tag{4.3}$$

where $\phi(A) \equiv \kappa^{\dagger}(I \otimes A)\kappa$ is in the predual space $\mathcal{B}_* \subset \mathcal{B}$ of all trace-class operators in $\mathcal{G}$, and $\phi_*(B) \equiv tr_{\mathcal{F}} \kappa B\kappa^{\dagger}$ is in $\mathcal{A}_* \subset \mathcal{A}$. The map ϕ is the Steinspring form of the general completely positive map $\mathcal{A} \to \mathcal{B}_*$, written in the eigen-basis $\{|n\rangle\}$ of $\mathcal{G} \subseteq l^2(\mathbb{N})$ of the density operator $\rho = \phi(I)$ as

$$\phi(A) = \sum_{m,n} |m\rangle \kappa_m^{\dagger}(I \otimes A)\kappa_n \langle n|, \quad A \in \mathcal{A} \tag{4.4}$$

where κ_n is the vector in $\mathcal{F} \otimes \mathcal{K}$ such that $\kappa = \sum_n \kappa_n \langle n|$. The dual operation ϕ_* is the Kraus form of the general completely positive map $\mathcal{B} \to \mathcal{A}_*$, given in this basis as

$$\phi_*(B) = \sum_{n,m} \langle n| B |m\rangle \, tr_{\mathcal{F}} \kappa_n \kappa_m^{\dagger}, \quad B \in \mathcal{B}. \tag{4.5}$$

It corresponds to the general form of the density operator

$$\theta_\phi = \sum_{m,n} |n\rangle\langle m| \otimes tr_{\mathcal{F}} \kappa_n \kappa_m^\dagger \tag{4.6}$$

for the entangled state Θ with the weak orthogonality property

$$tr_{\mathcal{F}\otimes\mathcal{K}} \kappa_n \kappa_m^\dagger = p_n \delta_n^m = \kappa_m^\dagger \kappa_n. \tag{4.7}$$

Definition 4.1 *The dual map $\phi_* : \mathcal{B} \to \mathcal{A}_*$ to a completely positive map $\phi : \mathcal{A} \to \mathcal{B}_*$, normalized as $tr_G \phi(I) = 1$, is called the quantum entanglement of the state $\rho = \phi(I)$ on $\mathcal{B}$ to the state $\sigma = \phi_*(I)$ on $\mathcal{A}$. The entanglement by $\phi(A) = \sigma^{1/2} A \sigma^{1/2}$ of the state $\rho = \sigma$ on the algebra $\mathcal{B} = \mathcal{A}$ given by the standard entangling operator $\kappa = \sigma^{1/2}$ is called standard.*

A compound state, playing the similar role as the joint input-output probability measures in classical systems, was introduced in [52] as explained in Sec.1. It corresponds to a particular diagonal type

$$\theta_\phi = \sum_n |n\rangle\langle n| \otimes tr_{\mathcal{F}} \kappa_n \kappa_n^\dagger$$

of the entangling map (4.5) in the eigen-basis(Schatten decomposition) of the density operator $\rho = \sum p_n |n\rangle\langle n|$. Therefore the entangled states, generalizing the compound state, also play the role of the joint probability measures.

The diagonal entanglements can be considered as a quantum correspondences of symbols $\{1, \cdots, n, \cdots\}$ to quantum states. The general entangled states Θ are described by the density operators θ_ϕ of the form (4.6) which is not necessarily diagonal in the eigen-representation of the density operator $\rho = \sum_n p_n |n\rangle\langle n|$. Such nondiagonal entangled states were called in [54] the quasicompound (q-compound) states, so we can call also the nondiagonal entanglement the quantum quasi-correspondence (q-correspondence) in contrast to the d-correspondences, described by the diagonal entanglements, giving rise to the d-compound states.

Take $tr_{\mathcal{F}} \kappa_n \kappa_n^\dagger \equiv \upsilon_n \upsilon_n^\dagger$, $\upsilon_n \in \mathcal{K}$. The density operator

$$\theta = \sum_n |n\rangle\langle n| \otimes \sigma_n, \quad \sigma_n = p_n \upsilon_n \upsilon_n^\dagger \tag{4.8}$$

define the compound states on $\mathcal{B} \otimes \mathcal{A}$, giving the quantum correspondences $n \mapsto |n\rangle\langle n|$ with the probabilities p_n. The entanglement with (4.8) is a diagonal entanglement such as

$$\phi_* (B) = \sum_n p_n \langle n|B|n\rangle \upsilon_n \upsilon_n^\dagger \tag{4.9}$$

whose dual is

$$\phi (A) = \sum_n p_n |n\rangle \upsilon_n^\dagger A \upsilon_n \langle n|. \tag{4.10}$$

These entanglements has the stronger orthogonality

$$tr_{\mathcal{F}} \kappa_n \kappa_m^\dagger = p_n \upsilon_n \upsilon_n^\dagger \delta_n^m, \tag{4.11}$$

for the amplitudes $\kappa_n \in \mathcal{F} \otimes \mathcal{K}$ of the decomposition $\kappa = \sum_n \kappa_n \langle n|$ in comparison with the weak orthogonality of κ_n in (4.6).

Definition 4.2 *The positive diagonal map*

$$\phi_* (B) = \sum_n \langle n|B|n\rangle \sigma_n \tag{4.12}$$

into the subspace of trace-class operation $\mathcal{K}$ with $tr_{\mathcal{G}} \phi_* (I) = 1$, is called quantum d-entanglement with the input probabilities $p_n = tr_{\mathcal{K}} \sigma_n$ and the output states $\omega_n = p_n^{-1} \sigma_n$, and the corresponding compound state (1.9) is called d-compound state. The d-entanglement is called c-entanglement and compound state is called c-compound if all density operators σ_n commute: $\sigma_m \sigma_n = \sigma_n \sigma_m$ for all m and n.

Note that due to the commutativity of the operators $B \otimes I$ with $I \otimes A$ on $\mathcal{G} \otimes \mathcal{K}$, one can treat the correspondences as the nondemolition measurements in $\mathcal{B}$ with respect to $\mathcal{A}$. So, the compound state is the state prepared for such measurements on the input $\mathcal{G}$. It coincides with the mixture of the states, corresponding to those after the measurement without reading the sent message. The set of all d-entanglements corresponding to a given Schatten decomposition of the input state ρ on A is obviously convex with the extreme points given by the pure elementary output states ω_n on $\mathcal{A}$, corresponding to a not necessarily orthogonal decompositions $\sigma = \sum_n \sigma_n$ into one-dimensional density operators $\sigma_n = p_n \omega_n$.

The orthogonal Schatten decompositions $\sigma = \sum_n p_n \omega_n$ correspond to the extreme points of c-entanglements which also form a convex set with mixed commuting ω_n for a given Schatten decomposition of σ. The orthogonal c-entanglements were used in [2] to construct a particular type of Accardi's transition expectations [1] and to define the entropy in a quantum dynamical system via such transition expectations[13].

Thus we classified the entangled states into three categories, namely, q-entangled state, d-entangled state and c-entangled state, and their rigorous expressions were given.

5 Mutual Entropy via Entanglements

Let us consider the entangled mutual entropy by means of the above three types compound states. We denote the quantum mutual entropy of the compound state Θ achieved by an entanglement $\phi_* : \mathcal{B} \to \mathcal{A}_*$ with the marginals

$$\Theta(B \otimes I) = tr_{\mathcal{G}} B\rho, \ \Theta(I \otimes A) = tr_{\mathcal{K}} A\sigma \tag{5.1}$$

by $I_\phi(\rho, \sigma)$ or $I_\phi(\mathcal{A}, \mathcal{B})$ and it is given as

$$I_\phi(\rho, \sigma) = tr\theta_\phi (\log \theta_\phi - \log(\rho \otimes \sigma)). \tag{5.2}$$

Besides this quantity describes an information gain in a quantum system $(\mathcal{A}, \sigma)$ via an entanglement ϕ_* with another system $(\mathcal{B}, \rho)$, it is naturally treated as a measure of the strength of an entanglement, having zero the value only for completely disentangled states (5.1), corresponding to $\theta_\phi = \rho \otimes \sigma$.

Definition 5.1 *The maximal quantum mutual entropy for a fixed state* σ

$$H_\sigma(\mathcal{A}) = \sup\{I_\phi(\mathcal{A}, \mathcal{B}); \phi_*(I) = \sigma\} \tag{5.3}$$

is called q-entropy of the state σ. *The differences*

$$\begin{aligned} H_\phi(\mathcal{B}|\mathcal{A}) &= H_\sigma(\mathcal{A}) - I_\phi(\mathcal{A}, \mathcal{B}), \\ D_\phi(\mathcal{B}|\mathcal{A}) &= S(\sigma) - I_\phi(\mathcal{A}, \mathcal{B}) \end{aligned}$$

are respectively called the q-conditional entropy on $\mathcal{B}$ *with respect to* $\mathcal{A}$ *and the degree of disentanglement for the compound state* ϕ.

$H_\phi(\mathcal{B}|\mathcal{A})$ is obviously positive, however $D_\phi(\mathcal{B}|\mathcal{A})$ has the positive maximal value $S(\sigma) = \sup\{D_\phi(\mathcal{B}|\mathcal{A}); \phi_*(I) = \sigma\}$ and can achieve also a negative value

$$\inf\{D_\phi(\mathcal{B}|\mathcal{A}); \phi_*(I) = \sigma\} = S(\sigma) - H_\sigma(\mathcal{A}) \tag{5.4}$$

for the entangled states [13], which is called the chaos degree in[31].

Let us consider $\mathcal{G}$ as a Hilbert space describing a quantum input system and $\mathcal{K}$ as its output Hilbert space. A quantum channel Λ^* sending each input state defined on $\mathcal{G}$ to an output state defined on $\mathcal{K}$. A deterministic quantum channel is given by a linear isometry $\Upsilon : \mathcal{G} \to \mathcal{K}$ with $\Upsilon^\dagger\Upsilon = I_0$ (I_0 is the identify operator in $\mathcal{G}$) such that each input state vector $\eta \in \mathcal{G}$, $\|\eta\| = 1$ is transmitted into an output state vector $\Upsilon\eta \in \mathcal{K}$, $\|\Upsilon\eta\| = 1$. The mixtures $\rho = \sum_n p_n\omega_n$ of the pure input states $\omega_n = \eta_n\eta_n^\dagger$ are sent into the mixtures $\sigma = \sum_n p_n\sigma_n$ with pure states $\sigma_n = \Upsilon\omega_n\Upsilon^\dagger$. A noisy quantum channel sends pure input states ω into mixed ones $\sigma = \Lambda^*\omega$ given by the dual of the following completely positive map Λ

$$\Lambda(A) = \Upsilon^\dagger(I_1 \otimes A)\Upsilon, \quad A \in \mathcal{A} \tag{5.5}$$

where Υ is a linear isometry from $\mathcal{G}$ to $\mathcal{F}_1 \otimes \mathcal{K}$, $\Upsilon^\dagger(I_1 \otimes I)\Upsilon = I_0$, and I_1 is the identity operator in a separable Hilbert space $\mathcal{F}_1$ representing the quantum noise. Each input mixed state $\rho \in B(\mathcal{G})$ is transmitted into the output state $\sigma = \Lambda^*\rho$ on $\mathcal{A} \subseteq B(\mathcal{K})$, which is given by the density operator

$$\sigma = tr_{\mathcal{F}_1}\Upsilon\rho\Upsilon^\dagger \equiv \Lambda^*\rho \in \mathcal{A}_*. \tag{5.6}$$

We apply the proceeding discussion of the entanglement to the above situation containing a channel Λ^*. For a given Schatten decomposition $\rho = \sum_n p_n|n\rangle\langle n|$ and the state $\sigma \equiv \Lambda^*\rho$,we can construct three entangled states of the proceeding section:

(1) q-entanglement ϕ_*^q and q-compound state θ_ϕ^q are given as

$$\begin{aligned} \phi_*^q(B) &= \sum_{n,m} \langle n \mid B \mid m\rangle\, tr_{\mathcal{F}}\kappa_n\kappa_m^\dagger \\ \theta_\phi^q &= \sum_{m,n} |n\rangle\langle m| \otimes tr_{\mathcal{F}}\kappa_n\kappa_m^\dagger \end{aligned}$$

with the marginals $\rho = \sum_n p_n|n\rangle\langle n|$, $\sigma \equiv \Lambda^*\rho = tr_{\mathcal{G}}\theta_\phi^q$ and $tr_{\mathcal{K}}\kappa_n\kappa_m^\dagger = p_n\omega_n\delta_n^m = \kappa_m^\dagger\kappa_n$ for $\omega_n = \Lambda^*|n\rangle\langle n|$. Let $\mathcal{E}_q$ be the convex set of all completely positive maps ϕ^q .

(2) d-entanglement ϕ_*^d and d-compound state θ_ϕ^d are given as

$$\begin{aligned}\phi_*^d(B) &= \sum_n \langle n \mid B \mid n\rangle \, tr_{\mathcal{F}} \kappa_n \kappa_n^\dagger \\ \theta_\phi^d &= \sum_n |n\rangle\langle n| \otimes tr_{\mathcal{F}} \kappa_n \kappa_n^\dagger\end{aligned}$$

with the same marginal conditions as (1). Let $\mathcal{E}_d$ be the convex set of all completely positive maps ϕ^d.

(3) c-entanglement ϕ_*^c and c-compound state θ_ϕ^c are same as those of (2) with commuting $\{\omega_n\}$. Let $\mathcal{E}_c$ be the convex set of all completely positive maps ϕ^c .

Now, let us consider the entangled mutual entropy and the capacity of quantum channel by means of the above three types of compound states.

Definition 5.2 *The mutual entropy $I_q(\rho, \Lambda^*)$ and the q-capacity $C_q(\Lambda^*)$ for a quantum channel Λ^* are defined by*

$$\begin{aligned}I_q(\rho, \Lambda^*) &= \sup\left\{S(\theta_\phi^q, \rho \otimes \Lambda^* \rho); \phi^q \in \mathcal{E}_q\right\}, \\ C_q(\Lambda^*) &= \sup\left\{I_q(\rho, \Lambda^*); \rho\right\}.\end{aligned} \tag{5.7}$$

The d-mutual entropy, the d-capacity and the c-mutual entropy, the c-capacity are defined as above using θ_ϕ^d and θ_ϕ^c, respectively.

Note that due to $\mathcal{E}_c \subseteq \mathcal{E}_d \subseteq \mathcal{E}_q$, we have the inequalities

$$\begin{aligned}I_q(\rho, \Lambda^*) &\geq I_d(\rho, \Lambda^*) \geq I_c(\rho, \Lambda^*), \\ C_q(\Lambda^*) &\geq C_d(\Lambda^*) \geq C_c(\Lambda^*)\end{aligned}$$

for a deterministic channel ($\Lambda^* = id$), the two lower mutual entropies coincide with the von Neumann entropy:

$$I_d(\rho, id) = -tr\rho\log\rho = I_c(\rho, id).$$

The capacity for such a channel is finite if $\mathcal{A}$ has a finite rank, $C_d(\Lambda^*) \leq \dim \mathcal{K}$. On the other hand, the q-mutual entropy can achieve the q-entropy

$$I_q(\rho, id) = -2tr\rho\log\rho$$

and its capacity is bounded by the dimension of the algebra $\mathcal{A}$, $C_q(\Lambda^*) \leq \dim \mathcal{A}$ which doubles the d-capacity $\dim\mathcal{K}$ when $\mathcal{A} = B(\mathcal{K})$. These equalities will be related to the work on entropy by Voiculescu [87].

Part II
Complexity in dynamics

6 Complexity and Chaos Degree in Information Dynamics

There exist several mathematical tools to describe chaotic aspects of natural or nonnatural phenomena such as (1) entropy and dynamical entropy, (2) Chaitin's complexity, (3) Lyapunov exponent, (4) fractal dimensions, (5) bifurcation, (6) ergodicity, (7)multiplicity [15, 61, 47, 3, 4, 39, 6, 5, 17, 26, 27, 84].

The author proposed Information Dynamics (ID for short) in 1991 to synthesize the dynamics of state change and the complexity of a system, and it is applied to several different fields such as quantum physics, fractal theory, quantum information and genetics[31].

A quantity measuring chaos in dynamical systems was defined by means of two complexities in ID, and it was called chaos degree. In particular, among several chaos degrees, the entropic chaos degree was introduced in [66] , and it is applied to logistic map[66] and other dynamical maps [34] to study their chaotic behaviors.

Here we briefly explain the concept of the complexity of ID in a bit simplified version (see[31, 56] for details).

Let $(\mathcal{A}, \mathfrak{S}, \alpha(G))$ be an input (or initial) system and $(\overline{\mathcal{A}}, \overline{\mathfrak{S}}, \overline{\alpha}(\overline{G}))$ be an output (or final) system. Here $\mathcal{A}$ is the set of all objects to be observed and $\mathfrak{S}$ is the set of all means for measurement of $\mathcal{A}$, $\alpha(G)$ is a certain evolution of system. Often we have $\mathcal{A} = \overline{\mathcal{A}}$, $\mathfrak{S} = \overline{\mathfrak{S}}$, $\alpha = \overline{\alpha}$. Therefore we claim

[Giving a mathematical structure to input and output triples
$\equiv$ Having a theory]

For instance, when $\mathcal{A}$ is the set $M(\Omega)$ of all measurable functions on a measurable space $(\Omega, \mathcal{F})$ and $\mathfrak{S}(\mathcal{A})$ is the set $P(\Omega)$ of all probability measures on Ω , we have usual probability theory, by which the classical dynamical system is described. When $\mathcal{A} = B(\mathcal{H})$, the set of all bounded linear operators on a Hilbert space $\mathcal{H}$, and $\mathfrak{S}(\mathcal{A}) = \mathfrak{S}(\mathcal{H})$, the set of density operators on $\mathcal{H}$, we have a quantum dynamical system.

Once an input and an output systems are set, the situation of the input system is described by a state, an element of $\mathfrak{S}$, and the change of the state is expressed by a mapping from $\mathfrak{S}$ to $\overline{\mathfrak{S}}$, called a channel, $\Lambda^* : \mathfrak{S} \to \overline{\mathfrak{S}}$ (sometimes $\mathfrak{S} \to \mathfrak{S}$). The channel Λ^* describes the dynamics of the system when $\mathcal{A} = \overline{\mathcal{A}}$, so that Λ^* depends on a certain parameter such as time and it may equal to α. The details of channels and their uses in physics and quantum communication are discussed in [2, 51].

Moreover, there exist two complexities in ID, which are axiomatically given as follows:

Let $(\mathcal{A}_t, \mathfrak{S}_t, \alpha^t(G^t))$ be the total system of $(\mathcal{A}, \mathfrak{S}, \alpha)$ and $(\overline{\mathcal{A}}, \overline{\mathfrak{S}}, \overline{\alpha})$, and let $C(\varphi) \in [0, \infty]$ be the complexity of a state φ and $T(\varphi; \Lambda^*) \in [0, \infty]$ be the transmitted complexity associated with the state change $\varphi \to \Lambda^*\varphi$. These complexities C and T are the quantities satisfying the following conditions:

(i) For any $\varphi \in \mathfrak{S}$,

$$C(\varphi) \geq 0,\ T(\varphi; \Lambda^*) \geq 0.$$

(ii) For any orthogonal bijection $j : ex\mathfrak{S} \to ex\mathfrak{S}$ (the set of all extreme points in $\mathfrak{S}$),

$$C(j(\varphi)) = C(\varphi),\ T(j(\varphi); \Lambda^*) = T(\varphi; \Lambda^*).$$

(iii) For $\Phi \equiv \varphi \otimes \psi \in \mathfrak{S}_t$,

$$C(\Phi) = C(\varphi) + C(\psi).$$

(iv) For any state φ and a channel Λ^*,

$$0 \leq T(\varphi; \Lambda^*) \leq C(\varphi).$$

(v) For the identity map "id" from $\mathfrak{S}$ to $\mathfrak{S}$. $T(\varphi; id) = C(\varphi)$.

Definition 6.1 : *Information Dynamics (ID) is defined by*
$\left(\mathcal{A}, \mathfrak{S}, \alpha(G); \overline{\mathcal{A}}, \overline{\mathfrak{S}}, \overline{\alpha}(\overline{G});\ \Lambda^*;\ C(\varphi), T(\varphi;\ \Lambda^*)\right)$
and some relations R among them.

Thus, in the framework of ID, we have to

(i) determine $\mathcal{A}, \mathfrak{S}, \alpha(G); \overline{\mathcal{A}}, \overline{\mathfrak{S}}, \overline{\alpha}(\overline{G})$ mathematically

(ii) choose Λ^* and R, and

(iii) define $C(\varphi)$, $T(\varphi;\Lambda^*)$.

Information Dynamics can be applied to the study of chaos in the following ways:

Definition 6.2 *(1)ψ is more chaotic than φ as seen from the reference system $\mathcal{S}$ if $C(\psi) \geq C(\varphi)$.*

(2)When φ changes to $\Lambda^*\varphi$, the degree of chaos associated to this state change(dynamics) Λ^* is given by

$$D(\varphi;\Lambda^*) = \inf\left\{\int_{\mathfrak{S}} C(\Lambda^*\omega)d\mu; \mu \in M(\varphi)\right\},$$

where $\varphi = \int_{\mathfrak{S}} \omega d\mu$ is a maximal extremal decomposition of φ and $M(\varphi)$ is the set of such measures. In some cases such that Λ^* is linear, this chaos degree $D(\varphi;\Lambda^*)$ can be written as $C(\Lambda^*\varphi) - T(\varphi;\ \Lambda^*)$.

In ID, several different topics can be treated from a common standpoint [31].

7 Entropic Complexity and Chaos Degree

Although there exist several complexities [64], one of the most fundamental pairs of C and T in quantum system is the von Neumann entropy and the mutual entropy, whose C and T are modified to formulate the entropic complexities such as ε-entropy (ε -entropic complexity) [54, 57, 61, 40], Kolmogorov-Sinai type dynamical entropy (entropic complexity)[4, 47, 39].

The concept of entropy was introduced and developed to study the following topics: irreversible behavior, symmetry breaking, amount of information transmission, chaotic properties of states, etc. Here we first show that the quantum entropy and the quantum mutual entropy are examples of our complexities C and T, respectively.

Let ρ be a state described by a density operator on a Hilbert space $\mathcal{H}$. The entropy of the state ρ was introduced by von Neumann [50, 70] as

$$S(\rho) = -tr\rho\log\rho$$

If $\rho = \sum_k p_k E_k$ is the Schatten decomposition (i.e., p_k is the eigenvalue of ρ and E_k is the one-dimensional projection associated with p_k, this decomposition is not unique unless every eigenvalue is non-degenerated) of ρ, then the von Neumann entropy takes the Shannon form

$$S(\rho) = -\sum_k p_k \log p_k,$$

because $\{p_k\}$ is a probability distribution. Therefore the von Neumann entropy contains the Shannon entropy as a special case.

For two states $\rho, \sigma \in \mathfrak{S}(\mathcal{H})$, the relative entropy [86, 7] is defined by

$$S(\rho,\sigma) = \begin{cases} tr\rho\,(\log\rho - \log\sigma) & (\rho \ll \sigma) \\ +\infty & (\text{otherwise}) \end{cases},$$

where $\rho \ll \sigma$ means that $tr\sigma A = 0 \Rightarrow tr\rho A = 0$ for any $A \geq 0$.

Let $\Lambda^* : \mathfrak{S}(\mathcal{H}) \to \mathfrak{S}(\overline{\mathcal{H}})$ be a channel and define the compound state by

$$\theta_E = \sum_k p_k E_k \otimes \Lambda^* E_k,$$

which expresses the correlation between the initial state ρ and the final state $\Lambda^*\rho$ for a linear (affine) channel[52, 53]. The mutual entropy [52, 54] for a state $\rho \in \mathfrak{S}(\mathcal{H})$ and a channel Λ^*, the amount of information transmitted from ρ to $\Lambda^*\rho$, is given by

$$\begin{aligned} I(\rho;\Lambda^*) &= \sup\{S(\theta_E, \rho\otimes\Lambda^*\rho); \{E_k\}\} \\ &= \sup\left\{\sum_k p_k S(\Lambda^* E_k, \Lambda^*\rho); \{E_k\}\right\}, \end{aligned} \tag{7.1}$$

where the supremum is taken over all Schatten decompositions. The above entropy and mutual entropy become a pair of our two complexities according to the following facts:

(1) The fundamental inequality of Shannon type [52, 63]:

$$0 \leq I(\rho;\Lambda^*) \leq \min\{S(\rho), S(\Lambda^*\rho)\}$$

because of $S(\Lambda^* E_k, \Lambda^*\rho) = S(\Lambda^*\rho) - \sum_k p_k S(\Lambda^* E_k) \leq S(\Lambda^*\rho)$ and the monotonicity[85, 70] of the relative entropy: $S(\Lambda^* E_k, \Lambda^*\rho) \leq S(E_k, \rho)$.

(2) $I(\rho; id) = S(\rho)$, which is proved as follows:
$I(\rho; id) = \sup\{\sum_k p_k S(E_k,\rho); \{E_k\}\}$
$= \sup\{\sum_k p_k (-S(E_k) - E_k \log \rho); \{E_k\}\} = S(\rho)$
because of $S(E_k) = 0$.

Thus the quantum entropy and the quantum mutual entropy satisfy all conditions of the complexity and the transmitted complexity, restepectively ; $C(\rho) = S(\rho)$, $T(\rho; \Lambda^*) = I(\rho; \Lambda^*)$.

In Shannon's communication theory in classical systems, ρ is a probability distribution $p = (p_k) = \sum_k p_k \delta_k$ and Λ^* is a transition probability $(t_{i,j})$, so that the Schatten decomposition of ρ is unique and the compound state of ρ and its output $\overline{\rho}$ $(\equiv \overline{p} = (\overline{p}_i) = \Lambda^* p)$ is the joint distribution $r = (r_{i,j})$ with $r_{i,j} \equiv t_{i,j} p_j$. Then the above complexities C and T become the Shannon entropy and mutual entropy, respectively;

$$C(p) = S(p) = -\sum_k p_k \log p_k,$$
$$T(p; \Lambda^*) = I(p; \Lambda^*) = \sum_{i,j} r_{i,j} \log \frac{r_{i,j}}{p_j \overline{p}_i}.$$

We can construct several other types of entropic complexities [64]. For instance, one pair of the complexities is

$$T(\rho; \Lambda^*) = \sup\left\{\sum_k p_k S(\Lambda^* \rho_k, \Lambda^* \rho); \rho = \sum_k p_k \rho_k\right\}, C(\rho) = T(\rho; id)$$

where $\rho = \sum_k p_k \rho_k$ is a finite decomposition of ρ and the supremum is taken over all such finite decompositions.

When the channel Λ^* is linear, since $S(\Lambda^* \rho) = -tr \Lambda^* \rho \log \Lambda^* \rho =$
$-tr(\sum_n p_n \Lambda^* E_n \log \Lambda^* \rho)$ for any Schatten decomposition $\{E_n\}$ of ρ and (7.1), we have

$$\begin{aligned} D(\rho; \Lambda^*) &= C(\Lambda^* \rho) - T(\rho; \Lambda^*) \\ &= S(\Lambda^* \rho) - I(\rho; \Lambda^*) \\ &= S(\Lambda^* \rho) - \sup\left\{tr\left(\sum_n p_n \Lambda^* E_n (\log \Lambda^* E_n - \log \Lambda^* \rho)\right); \{E_n\}\right\} \\ &= \inf\left\{\sum_n p_n S(\Lambda^* E_n); \{E_n\}\right\} \end{aligned} \tag{7.2}$$

The above quantity $D(\rho; \Lambda^*)$ is interprated as the complexity produced through the channel Λ^*. We apply this quantity $D(\rho; \Lambda^*)$ to study quantum

chaos even when the channel describing the dynamics is not linear. $D(\rho;\Lambda^*)$ is called the entropic chaos degree in the sequel of this paper.

In order to contain more general dynamics such as in continuous systems, we define the entropic chaos degree in C*-algebraic terninology. This setting will not be used in the sequel application, but for mathematical completeness we will discuss the C*-algebraic setting.

Let $(\mathcal{A},\mathfrak{S})$ be an input C* system and $(\overline{\mathcal{A}},\overline{\mathfrak{S}})$ be an output C* system; namely, $\mathcal{A}$ is a C* algebra with unit I and $\mathfrak{S}$ is the set of all states on $\mathcal{A}$. We assume $\overline{\mathcal{A}}=\mathcal{A}$ for simlicity. For a weak* compact convex subset $\mathcal{S}$ (called the reference space) of $\mathfrak{S}$, take a state φ from the set $\mathcal{S}$ and let

$$\varphi=\int_{\mathcal{S}}\omega d\mu_{\varphi}$$

be an extremal orthogonal decomposition of φ in $\mathcal{S}$, which describes the degree of mixture of φ in the reference space $\mathcal{S}$. The measure μ_{φ} is not uniquely determined unless $\mathcal{S}$ is the Schoque simplex, so that the set of all such measures is denoted by $M_{\varphi}(\mathcal{S})$. The entropic chaos degree with respect to $\varphi\in\mathcal{S}$ and a channel Λ^* is defined by

$$D^{\mathcal{S}}(\varphi;\Lambda^*)\equiv\inf\left\{\int_{\mathcal{S}}S^{\mathcal{S}}(\Lambda^*\varphi)\,d\mu_{\varphi};\mu_{\varphi}\in M_{\varphi}(\mathcal{S})\right\} \tag{7.3}$$

where $S^{\mathcal{S}}(\Lambda^*\varphi)$ is the mixing entropy of a state φ in the reference space $\mathcal{S}$ [62]. When $\mathcal{S}=\mathfrak{S}$, $D^{\mathcal{S}}(\varphi;\Lambda^*)$ is simply written as$D(\varphi;\Lambda^*)$. This $D^{\mathcal{S}}(\varphi;\Lambda^*)$ contains the classical chaos degree and the quantum one (7.2). The claasical entropic chaos degree is the case that $\mathcal{A}$ ia abelian and φ is the probability disribution of a orbit generated by a dynamics (channel) Λ^*; $\varphi=\sum_k p_k\delta_k$, where δ_k is the delta measure such as $\delta_k(j)\equiv\begin{cases}1 & (k=j)\\ 0 & (k\neq j)\end{cases}$. Then the claasical entropic chaos degree is

$$D_c(\varphi;\Lambda^*)=\sum_k p_k S(\Lambda^*\delta_k) \tag{7.4}$$

with the Shannon entropy S.

8 Algorithm of Chaos Degree

Algorithmically these chaos degrees D_c and D_q for classical and quantum dynamics are set as follows: A dynamics of a state is given by a channel $F^*($

F_t^*) or a mapping F (F_t) on $I \equiv [a,b]^{\mathbf{N}} \subset \mathbf{R}^{\mathbf{N}}$ or a certain Hilbert space $\mathcal{H}$, for instance, $\varphi_t = F_t^* \varphi_0$, $\frac{dx}{dt} = F(x)$ with $x \in I$ or $\mathcal{H}$. For a state $\varphi^{(n)}$ at the time (steps) n after a certain time (steps) m , let Λ^* be the channel properly defined by a given dynamics F^* or F. Note that in some cases $\Lambda^* = F^*$, but generally $\Lambda^* \neq F^*$. We will briefly discuss how to compute the entropic chaos degrees for a classical dynamics and a quantum dynamics.

(1) *Classical Chaos Degree* D_c : For a map F on $I \equiv [a,b]^{\mathbf{N}} \subset \mathbf{R}^{\mathbf{N}}$ with $x_{n+1} = F(x_n)$ (a difference equation), let $I \equiv \bigcup_k A_k$ be a finite partation with $A_i \cap A_j = \emptyset$ $(i \neq j)$. The state $\varphi^{(n)}$ of the orbit determined by the difference equation is defined by the probabilty distribution $\left(p_i^{(n)}\right)$, that is, $\varphi^{(n)} = \sum_i p_i^{(n)} \delta_i$, where for an initial value $x \in I$ and the characteristic function 1_A

$$p_i^{(n)} \equiv \frac{1}{m+1} \sum_{k=n}^{m+n} 1_{A_i}\left(F^k x\right). \tag{8.1}$$

When the initial value x is distributed due to a measure υ on I, the above $p_i^{(n)}$ is given as

$$p_i^{(n)} \equiv \frac{1}{m+1} \int_I \sum_{k=n}^{m+n} 1_{A_i}\left(F^k x\right) d\nu. \tag{8.2}$$

The joint distribution $\left(p_{ij}^{(n,n+1)}\right)$ between the time n and $n+1$ is defined by

$$p_{ij}^{(n,n+1)} \equiv \frac{1}{m+1} \sum_{k=n}^{m+n} 1_{A_i}\left(F^k x\right) 1_{A_j}\left(F^{k+1} x\right) \tag{8.3}$$

or

$$p_{ij}^{(n,n+1)} \equiv \frac{1}{m+1} \int_I \sum_{k=n}^{m+n} 1_{A_i}\left(F^k x\right) 1_{A_j}\left(F^{k+1} x\right) d\nu. \tag{8.4}$$

Then the channel Λ_n^* at n is determined by

$$\Lambda_n^* \equiv \left(\frac{p_{ij}^{(n,n+1)}}{p_i^{(n)}}\right) \Longrightarrow \varphi^{(n+1)} = \Lambda_n^* \varphi^{(n)}, \tag{8.5}$$

and the chaos degree is given by

$$D_c\left(\varphi^{(n)};\Lambda_n^*\right)=\sum_i p_i^{(n)}S(\Lambda_n^*\delta_i)=\sum_{i,j}p_{ij}^{(n,n+1)}\log\frac{p_i^{(n)}}{p_{ij}^{(n,n+1)}}. \tag{8.6}$$

This classical chaos degree was applied to several dynamical maps such logistic map, Baker's transformation and Tinkerbel map, and it could explain their chaotic characters[66, 34]. Our chaos degree has several merits compared with usual measures such as Lyapunov exponent.

(2) *Quantum chaos degree* D_q : Here we explain the entropic chaos degree of a quantum system described by a density operator. Let F^* be a channel sending a state to a state and ρ be an intial state. After time n, the state is $F^{*n}\rho$, whose Schatten decomposition is denoted by $\sum_k \lambda_k^{(n)}E_k^{(n)}$. Then define a channel Λ_m^* on $\otimes_1^m\mathcal{H}$ by

$$\Lambda_m^*\sigma=F^*\sigma\otimes\cdots\otimes F^{*m}\sigma,\ \sigma\in\mathfrak{S}(\mathcal{H}), \tag{8.7}$$

from which the entropic chaos degree (7.3) is written as

$$D_q\left(\rho;\Lambda_m^*\right)=\inf\left\{\frac{1}{m}\sum_k\lambda_k^{(n)}S\left(\Lambda_m^*E_k^{(n)}\right);\left\{E_k^{(n)}\right\}\right\}, \tag{8.8}$$

where the infimum is taken over all Schatten decompositions of $F^{*n}\rho$.

The quantum entropic chaos degree is applied to the analysis of quantum spin system[32] and quantum Baker's type transformation[35], and we could measure the chaos of these systems.

Part III
Computaional Complexity

When we solve a problem with the input size n, like a sequence composed of n letters of 0 and 1, under a certain algorithm, and the time (steps) to solve this problem by computer is in polynominal order of the size n, the algorithm is called "good" algorithm and the problem is said to belong to P (polynominal) class. Such a problem is one to be recognized in polynominal time by a deterministic Turing machine. On the other hand, the problem to be recognized in polynominal time by a non-deterministic Turing machine is called NP problem. A NP problem can be also understood as the problem whose solution can not be obtained in polynominal time, but a candidacy of the solutions can be examined in polynominal time to be a real solution of this problem or not. One of fundamental problems of computational complexity is whether there exists an algorithm to solve the NP problem in polynominal time; namely, NP=P or not. It is known [74] that there exist the most difficult NP problems in NP class, called NP complete problem, and they are all equivalent. There are several NP complete problems such as SAT(satisfiability) problem, Salesman problem and Napsack problem.

In [69], we showed that SAT problem can be solved in plynonimal time if a superposition of two orthogonal vectors is detected experimentally. We will explain basic part of our result in this paper.

9 SAT Problem

Let $X \equiv \{x_1, \cdots, x_n\}$ be a set. Then x_k and its negation $\overline{x}_k$ $(k = 1, 2, \cdots, n)$ are called literals and the set of all such literals is denoted by $X' = \{x_1, \overline{x}_1, \cdots, x_n, \overline{x}_n\}$. The set of all subsets of X' is denoted by $\mathcal{F}(X')$ and an element $C \in \mathcal{F}(X')$ is called a clause. We take a truth assignment to all variables x_k. If we can assign the truth value to at least one element of C, then C is called satisfiable. When C is satisfiable, the truth value $t(C)$ of C is regarded as true, otherwise, that of C is false. Take the truth values as "true$\leftrightarrow$ 1, false$\leftrightarrow$ 0". Then

C is satisfiable iff t(C)=1.

Let $L = \{0, 1\}$ be a Boolean lattice with usual join $\vee$ and meet $\wedge$, and $t(x)$ be the truth value of a literal x in X. Then the truth value of a clause

C is written as $t(C) \equiv \vee_{x \in C} t(x)$. Moreover the set $\mathcal{C}$ of all clauses C_j $(j = 1, 2, \cdots m)$ is called satisfiable iff the meet of all truth values of C_j is 1; $t(\mathcal{C}) \equiv \wedge_{j=1}^{m} t(C_j) = 1$. Thus the SAT problem is written as follows:

Definition 9.1 *SAT Problem: Given a set* $X \equiv \{x_1, \cdots, x_n\}$ *and a set* $\mathcal{C} = \{C_1, C_2, \cdots, C_m\}$ *of clauses, determine whether* $\mathcal{C}$ *is satisfiable or not.*

That is, this problem is to ask whether there exsits a truth assignment to make $\mathcal{C}$ satisfiable.

It is known[74] in usual algorithm that it is polynomial time to check the satisfiability only when a specific truth assignment is given, but we can not determine the satisfiability in polynomial time when an assignment is not specified.

10 Quantum Algorithm of SAT

Let 0 and 1 of the Boolean lattice L be denoted by the vectors $|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ in the Hilbert space $\mathbf{C}^2$, respectively. That is, the vector $|0\rangle$ corresponds to falseness and $|1\rangle$ does to truth.

As we explained in the previous section, an element $x \in X$ can be denoted by 0 or 1, so by $|0\rangle$ or $|1\rangle$. In order to describe a clause C with at most n length by a quantum state, we need the n-tuple tensor product Hilbert space $\mathcal{H} \equiv \otimes_1^n \mathbf{C}^2$. For instance, in the case of $n = 2$, given $C = \{x_1, x_2\}$ with an assignment $x_1 = 0$ and $x_2 = 1$, then the corresponding quantum state vector is $|0\rangle \otimes |1\rangle$, so that the quantum state vector describing C is generally written by $|C\rangle = |x_1\rangle \otimes |x_2\rangle \in \mathcal{H}$ with $x_k = 0$ or 1 (k=1,2).

The quantum computation is performed by a unitary gate constructed from several fundamental gates such as Not gate, Controlled-Not gate, Controlled-Controlled Not gate[20, 68]. Once $X \equiv \{x_1, \cdots, x_n\}$ and $\mathcal{C} = \{C_1, C_2, \cdots, C_m\}$ are given, the SAT is to find the vector $|f(\mathcal{C})\rangle \equiv \wedge_{j=1}^{m} \vee_{x \in C_j} t(x)$, where $t(x)$ is $|0\rangle$ or $|1\rangle$ when $x = 0$ or 1, respectively, and $t(x) \wedge t(y) \equiv t(x \wedge y)$, $t(x) \vee t(y) \equiv t(x \vee y)$.

We consider the quantum algorithm for the SAT problem. Since we have n variables x_k $(k = 1, \cdots n)$ and a quantum computation produces some dust bits, the assignments of the n variables and the dusts are represented by n

qubits and l qubits in the Hilbert space $\otimes_1^n \mathbf{C}^2 \otimes_1^l \mathbf{C}^2$. Moreover the resulting state vector $|f(\mathcal{C})\rangle$ should be added, so that the total Hilbert space is

$$\mathcal{H} \equiv \otimes_1^n \mathbf{C}^2 \otimes_1^l \mathbf{C}^2 \otimes \mathbf{C}^2.$$

Let us start the quantum computation of SAT problem from an initial vector $|v_0\rangle \equiv \otimes_1^n |0\rangle \otimes_1^l |0\rangle \otimes |0\rangle$ when $\mathcal{C}$ contains n Boolean variables $x_1, \cdots x_n$. We apply the discrete Fourier transformation denoted by $U_F \equiv \otimes_1^n \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ to the part of the Boolean variables of the vector $|v_0\rangle$, then the resulting state vector becomes

$$|v\rangle \equiv U_F \otimes_1^{l+1} I |v_0\rangle = \frac{1}{\sqrt{2^n}} \otimes_1^n (|0\rangle + |1\rangle) \otimes_1^l |0\rangle \otimes |0\rangle,$$

where I is the identity matrix in $\mathbf{C}^2$. This vector can be written as

$$|v\rangle = \frac{1}{\sqrt{2^n}} \sum_{x_1,\cdots,x_n=0}^{1} \otimes_{j=1}^n |x_j\rangle \otimes_1^l |0\rangle \otimes |0\rangle.$$

Now, we perform the quantum computer to check the satisfiability, which will be done by a unitary operator U_f properly constructed by unitary gates. Then after the computation by U_f, the vector $|v\rangle$ goes to

$$\begin{aligned} |v_f\rangle &\equiv U_f |v\rangle = \frac{1}{\sqrt{2^n}} \sum_{x_1,\cdots,x_n=0}^{1} U_f \otimes_{j=1}^n |x_j\rangle \otimes_1^l |0\rangle \otimes |0\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x_1,\cdots,x_n=0}^{1} \otimes_{j=1}^n |x_j\rangle \otimes_{i=1}^l |y_i\rangle \otimes |f(x_1,\cdots,x_n)\rangle, \end{aligned}$$

where $f(x_1,\cdots,x_n) \equiv f(\mathcal{C})$ because $\mathcal{C}$ contains $x_1, \cdots x_n$, and $|y_i\rangle$ are the dust bits produced by the computation. As we will explain in an example below, the unitary operator U_f is concretely constructed.

For the case $X = \{x_1, x_2, x_3\}$ and $\mathcal{C} = \{\{x_1\}, \{x_2, x_3\}, \{x_1, \overline{x}_3\}, \{\overline{x}_1, \overline{x}_2, x_3\}\}$, the resulting state $|f(x_1, x_2, x_3)\rangle$ is written as

$$|f(x_1, x_2, x_3)\rangle = |x_1\rangle \wedge (|x_2\rangle \vee |x_3\rangle) \wedge (|x_1\rangle \vee |\overline{x}_3\rangle) \wedge (|\overline{x}_1\rangle \vee |\overline{x}_2\rangle \vee |x_3\rangle)$$

In the quantum computation, it is not necessary to substitute all values of x_j $(j = 1, 2, 3)$ as the classical computation, we have only to use a unitary operator U_f for the computation of $|f(x_1, x_2, x_3)\rangle$. This unitary operator U_f is constructed as follows: Let U_{NOT}, U_{CN} and U_{CCN} be Not gate on $\mathbf{C}^2$, Controlled-Not gate on $\mathbf{C}^2 \otimes \mathbf{C}^2$ and Controlled-Controlled-Not gate on $\mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \mathbf{C}^2$, respectively, which are given by

$$
\begin{aligned}
U_{NOT} &= |0\rangle\langle 1| + |1\rangle\langle 0| \\
U_{CN} &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes (|0\rangle\langle 1| + |1\rangle\langle 0|) \\
U_{CCN} &= |0\rangle\langle 0| \otimes |0\rangle\langle 0| \otimes I + |0\rangle\langle 0| \otimes |1\rangle\langle 1| \otimes I + |1\rangle\langle 1| \otimes (|0\rangle\langle 0| \otimes |1\rangle\langle 0|)
\end{aligned}
$$

Then the unitary operator U_f is determined by the combination of the above three unitaries as

$$U_f \equiv U_{36} U_{35} \cdots U_2 U_1,$$

where, for instance,

$$
\begin{aligned}
U_1 &\equiv |0\rangle\langle 0| \otimes_1^{23} I + |1\rangle\langle 1| \otimes_1^{2} I \otimes (|0\rangle\langle 1| + |1\rangle\langle 0|) \otimes_1^{20} I \\
U_2 &\equiv I \otimes |0\rangle\langle 0| \otimes_1^{22} I + I \otimes |1\rangle\langle 1| \otimes_1^{2} I \otimes (|0\rangle\langle 1| + |1\rangle\langle 0|) \otimes_1^{19} I \\
U_3 &\equiv \otimes_1^{2} I \otimes |0\rangle\langle 0| \otimes_1^{21} I + \otimes_1^{2} I \otimes |1\rangle\langle 1| \otimes_1^{2} I \otimes (|0\rangle\langle 1| + |1\rangle\langle 0|) \otimes_1^{18} I
\end{aligned}
$$

and other $U_4, \cdots, U_{36}$ are similarly constructed (see the computation diagram 1). In this case, we need 20 dust bits (the number of the dust bits needed in a general case is counted in the next section), so that U_f is operated on the Hilbert space $\otimes_1^{24} \mathbf{C}^2$.

Starting from the initial vector $|v_0\rangle \equiv \otimes_1^{3} |0\rangle \otimes_1^{20} |0\rangle \otimes |0\rangle$, the final vector is

$$
\begin{aligned}
|v_f\rangle &= U_{36} \cdots U_1 U_F |v_0\rangle = U_f U_F |v_0\rangle \\
&= \frac{1}{\sqrt{2^3}} (|0,0,0,0,1,1,0,1,0,1,0,0,0,1,1,0,0,0,1,1,1,0,1;0\rangle \\
&\quad + |1,0,0,1,1,1,0,0,0,1,1,0,0,1,1,1,0,0,1,1,1,0,1;0\rangle \\
&\quad + |0,1,0,0,0,1,1,1,0,1,0,1,0,1,1,0,1,0,1,1,1,0,1;0\rangle \\
&\quad + |0,0,1,0,1,0,1,1,1,0,0,0,0,0,1,0,1,0,0,1,0,0,0;0\rangle \\
&\quad + |1,1,0,1,0,1,1,0,0,1,1,1,1,1,0,1,1,1,1,1,0,1,0;0\rangle
\end{aligned}
$$

$$+|1,0,1,1,1,0,1,0,1,1,1,0,0,0,1,1,1,1,1,1,1,1,1;1\rangle$$
$$+|0,1,1,0,0,0,1,1,1,0,0,1,0,0,1,0,1,0,0,1,0,0,0;0\rangle$$
$$+|1,1,1,1,0,0,1,0,1,1,1,1,1,0,1,1,1,1,1,1,1,1,1;1\rangle),$$

where we used the notation

$$|x_1,x_2,x_3,y_1,\cdots,y_{20};f(x_1,x_2,x_3)\rangle \equiv \otimes_{j=1}^{3}|x_j\rangle \otimes_{i=1}^{20}|y_i\rangle \otimes |f(x_1,x_2,x_3)\rangle$$

Go back to general discussion. The final step to check the satisfiability of $\mathcal{C}$ is to apply the projection $E \equiv \otimes_1^{n+l} I \otimes |1\rangle\langle 1|$ to the state $|v_f\rangle$, mathematically equivalent , to compute the value $\langle v_f|E|v_f\rangle$. If the vector $E|v_f\rangle$ exists or the value $\langle v_f|E|v_f\rangle$ is not 0, then we conclude that $\mathcal{C}$ is satisfiable. The value of $\langle v_f|E|v_f\rangle$ corresponds to that of the ramdom algorithm as we will see in an example of the next section and it may or may not be obtained in polynominal time. Let us consider an operator V_θ, given by

$$V_\theta \equiv \otimes_1^{n+l}(A|0\rangle\langle 0| + B|1\rangle\langle 1|) \otimes e^{i\theta f(C)} I,$$

and apply it to the vector $|v_f\rangle$, where $A \equiv \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $B \equiv \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ and θ is a certain constant describing the phase of the vector $|f(\mathcal{C})\rangle$. The resulting vector is the superposition of two vectors with some constants α, β such as

$$V_\theta|v_f\rangle = \frac{1}{\sqrt{2^{n+l}}} \otimes_1^{n+l}(|0\rangle + |1\rangle) \otimes (\alpha|0\rangle + \beta e^{i\theta}|1\rangle),$$

one of which is polarized with θ and another is non-polarized. The existence of the mixture of two vectors $|0\rangle$ and $e^{i\theta}|1\rangle$ is a charaeteritic point of quantum computation, which implies the satisfiability. Thus the number of steps for the quantum algorithm of the SAT problem is easily checked to be in polynominal order of n [69].

Part IV
Information Genetics

11 Entropy Evolution Rate

Genome sequence carries information as an order of four bases, and the information is transmitted to m-RNA, which makes a protein as a sequence of amino acids by a help of t-RNA.

In information theory, the concept of information has two aspects, one of which expresses the amount of complexity of a whole system like a sequence itself and another does the structure of the system(or message) such as the rule stored in the order of sequence[31]. From Shannon's philosophy, a system has the larger complexity, the system carries the larger information, from which the information of a whole system has been expressed by the entropy. The structure of the system is studied in the field named "coding theory", that is, how to code the messages is essential in communication of information.

Pioneering works for application of information theory to genome sequence were done by Smith[82]and Gatlin[24], since then few works have been appeared along this line. In 1989 [55], I introduced a measure representing the difference of two genome or amino acid sequences, which is called the entropy evolution rate and has been used to make phylogenetic trees[55, 46]. The coding theory was applied to the study of genome sequences in order to examine the coding structure of several species[58].

Let A and B be amino acid or base sequences. When they are considered to be close each other, for instance, they specify an identical protein, we first have to align these sequences by inserting a gap "$*$", whose arrangement is called the alignment of sequences[78, 49, 60]. As an example, take two sequences A and B given as

$$A: \text{a c b a c d}$$
$$B: \text{a d b c a c b}$$

Then the aligned sequences become

$$A: \text{a c b} * \text{a c d}$$
$$B: \text{a d b c a c b}$$

After the alignment, two sequences have the same length. Take two aligned sequences A and B having the length n given by A=(a_1, a_2, $\cdots$, a_n), B=(b_1, b_2, $\cdots$, b_n), where a_i, b_i are the gap $*$ or an amino acid for an amino acid sequence or a base for a base sequence. There are 21 events (20 amino acids and $*$) in an amino acid sequence and 5 events (4 bases and $*$) in a base sequence. Therefore, in an aligned sequence, the occurrence probability of each amino acid (resp. base) is associated, and it is denoted by p_k for k-th amino acid (resp. base), where $0 \leq k \leq 20$ (resp. $0 \leq k \leq 4$) and "0" corresponds to the gap. Then the entropy (information) carried by the amino acid (resp. base) sequence A is defined as

$$S(A)(\text{or } S(p)) = -\sum_k p_k \log p_k$$

where p denotes the probability distribution (p_k). Similarly, there exists the event system $(B, q \equiv (q_k))$ for the amino acid (or base) sequence B, and its entropy is denoted $S(B)$ or $S(q)$. Through the alignment, we can find the correspondence between the amino acid (resp. base) of A and that of B, which enables to make the compound event system $(A \times B, r)$ of A and B. Here r is the joint probability distribution between A and B, so that it satisfies $\sum_k r_{jk} = p_j$ and $\sum_k r_{jk} = q_k$.

The most important information measure in Shannon's communication theory is the mutual entropy (information) expressing the amount of information transmitted from (A, p) to (B, q), which is defined as follows:

$$I(A, B) = \sum_{j,k} r_{jk} \log \frac{r_{jk}}{p_j q_k}.$$

Using the entropy and the mutual entropy, an quantity measuring the similarity between A and B was introduced as

$$r(A, B) = \frac{1}{2}\left\{\frac{I(A, B)}{S(A)} + \frac{I(A, B)}{S(B)}\right\},$$

which was called the symmetrized entropy ratio or the entropy evolution rate in [55]and it takes the value 0 when A and B are completely different and 1 when they are identical. The minus of this rate from 1 indicates the difference between A and B. We here call it the entropy evolution rate, and it is denoted by $\rho(A, B)$:

$$\rho(A,B) = 1 - r(A,B).$$

Using this rate, we can construct a genetic matrix and write a phylogenetic tree of species[55, 46]. Note that a similar measure providing the difference between A and B can be defined as

$$\rho'(A,B) = 1 - \frac{I(A,B)}{S(A) + S(B) - I(A,B)},$$

but this dose not have a precise meaning from the information theoretical point of view.

An application of this rate to the variation of HIV virus for six patients reported by [88, 29, 44, 37]is discussed in [75].

12 Code Structure of Genes

When we send an information (a series of messages), we have to process the messages in proper forms so as to correctly and quickly send the information to a receiver. It is the coding theory that teaches us how to process the messages properly. There are many ways to encode the messages in communication processes. We shall explain some of such codings and their use to the study of genome sequences.

Let $i = (i_1, i_2, \cdots, i_k)$ be a properly processed information sequence. In order to send the symbol i to a receiver correctly, that is, to avoid some noise and loss in the course of information transmission, we have to add some redundancy (parity check symbol) $p = (p_1, p_2, \cdots, p_{n-k})$ to the information symbol i. This redundancy p detects or corrects the errors in the communication process. The whole code-word now becomes

$$x = (i_1, i_2, \cdots, i_k, p_1, p_2, \cdots, p_{n-k}).$$

The above x is called a systematic code, and to make the systematic code x from the information symbol i is called a coding. A coding is realized by a Galois group $GF(q)$ with a primary number q and a certain parity check p. When the relation between i and p is linear, the code so obtained is called a linear code. Among the linear codes, there are the block code such as cyclic code and BCH code and the convolutional code such as self-orthogonal code

and Iwadare code. Each code has its own parity check correcting the error such as random error, burst error and bite error. We do not go into the details of the coding theory here, but we explain how to use the coding technique to examine the code structure of genome sequences.

When we like to know the code structure of a species, an organism, a special part of a genome sequence indicating a protein or a set of these objects, we rewrite a base sequence of an object into the sequence of the symbols of $GF(2^2)$ because we have four bases, and we apply several coding methods to the symbol sequence and get the coded symbol sequence (systematic code), then we write it back the coded base sequence. This process is written as follows:

$$\text{Base sequence } A \Longrightarrow \text{Symbol sequence } A_s$$
$$\Longrightarrow \text{Coded symbol sequence } A_s^C \Longrightarrow \text{Coded base sequence } A^C$$

In order to know the common code structure of the sequences $A_1, A_2, \cdots, A_n$, we use the following index obtained from the entropy evolution rate and a coding C applied to the sequences:

$$D_C = \frac{\left\{\sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\left|\rho(A_i, A_j) - \rho\left(A_i^C, A_j^C\right)\right|\right\}}{{}_{\mathrm{n}}\mathrm{C}_2},$$

where ${}_{\mathrm{n}}\mathrm{C}_2$ is the combination 2 out of n, that is, ${}_{\mathrm{n}}\mathrm{C}_2 = \frac{n(n-1)}{2}$ and A_i is an amino acid sequence or a base sequence. Note that when A_i is originally an amino acid sequence, we first translate it the corresponding base sequence and take the above procedure, then we convert the coded base sequence to the coded amino acid sequence. If this index D_C is close to 0, then a common code structure of the group $\{A_1, A_2, \cdots, A_n\}$ is close to the structure of the code C used.

We studied the code structure of Vertebrate, Onco virus and HIV virus by means of the structure index D_C. We used some parts of the base sequence for each organisms; MDH, LDH, hemoglobin α, β for Vertebrate; pol, env, gag for Onco and HIV virus. Then we obtained the following results:

(1) Vertebrate has a similar code structure of the convolutional code with high ability correcting the burst errors like the codes named UI, ZI, and the code structure of hemoglobin α is closest to that of the artificial codes.

(2) Onco virus has a similar code structure of the cyclic code with the burst error correction (C2) or the self-orthogonal code (TB,VD), so that it does not have so high ability correcting the errors.

(3) HIV virus has a similar code structure of the cyclic code (C1) or the self-orthogonal code with the random error correction (TA) , so that the ability correcting the errors is low.

(4) In Onco and HIV virus, the pol protein has the closest code structure of the artificial codes.

The structure index is applied to the study of the variation and the condition of the patients having the HIV infection in [83].

References

[1] L. Accardi, Noncommutative Markov chains, International School of Math. Phys., Camerino, pp.268-295, 1974.

[2] L.Accardi and M.Ohya, Compound channels, transition expectations and liftings, Appl. Math. Optim., **39**, pp.33-59, 1999.

[3] L.Accardi, M.Ohya and N.Watanabe, Dynamical entropy through Markov chain, Open Systems and Information Dynamics, **4**, No.1, pp71-87, 1997.

[4] L.Accardi, M.Ohya and N.Watanabe, Note on quantum dynamical entropy, Reports on Mathematical Physics, **38**, pp.457-469, 1996.

[5] R.Alicki, Quantum geometry of noncommutative Bernoulli shifts, Banach Center Publications, Mathematics Subject Classification 46L87, 1991.

[6] S.Akashi, The asymptotic behavior of ε-entropy of a compact positive operator, J.Math.Anal.Appl., **153**, pp.250-257, 1990.

[7] H.Araki, Relative entropy for states of von Neumann algebras, Publications in RIMS Kyoto University, **11**, pp.809-833, 1976.

[8] K.T Alligood, T.D.Sauer and J.A.Yorke, *Chaos-An Introduction to Dynamical Systems-*, Textbooks in Mathematical Sciences, Springer, 1996.

[9] V.P. Belavkin, Quantum filtering of Markov signals with white quantum noise, in "Quantum Communications and measurement", Plenum Press, pp.381–391, 1995.

[10] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W.K. Wootters, Teleporting an unknown quantum state via Dual Classical and Einstein-Podolsky-Rosen channels, Phys. Rev. Lett., **70**, pp.1895-1899, 1993.

[11] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J.A. Smolin, W.K. Wootters, Purification of noisy entanglement and faithful teleportation via noisy channels, Phys. Rev. Lett., **76** , pp.722-725, 1996.

[12] P.Billingsley, *Ergodic Theory and Information,* Wiley, NewYork, 1965.

[13] V.P. Belavkin and M. Ohya, Quantum entanglement and entangled mutual entropy, SUT preprint.

[14] V.P. Belavkin and P.L. Stratonovich, Optimization of processing of quantum signals according to an information Criterion, Radio Eng. Electron. Phys., **18**, No.9, pp.1839-1844, 1973.

[15] A.Connes, H.Narnhofer and W.Thirring, Dynamical entropy of C*-algebras and von Neumann algebras, Communications in Mathematical Physics, **112**, pp.691-719, 1987.

[16] A.Connes and E.Størmer, Entropy for automorphisms of II_1 von Neumann algebras, Acta Mathematica, **134**, pp.289-306, 1975.

[17] R.L.Devaney, An Introduction to Chaotic dynamical Systems, Benjamin, 1986.

[18] D.Deutsch, Quantum theory, the Church-Turing principle and the universal quantum computer, Proc. of Royal Society of London series A, **400**, pp.97-117, 1985.

[19] D. Deutsch and R. Jozsa, Rapid solution of problems by quantum computation, Proc. of Royal Society of London series A, **439** , pp.553-558, 1992.

[20] A.Ekert and R.Jozsa, Quantum computation and Shor's factoring algorithm, Reviews of Modern Physics, **68** No.3,pp.733-753, 1996.

[21] A. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett, **67**, pp.661-663, 1991.

[22] G.G.Emch, Positivity of the K-entropy on non-abelian K-flows, Z. Wahrscheinlichkeitstheorie Verw. Gebiete, **29**, pp.241-252, 1974.

[23] R.Feymann, Quantum mechanical computer, Optics News, **11**, pp.11-20, 1985.

[24] L.L.Gatlin, Information Theory and The living System, Columbia Univ. Press, 1972.

[25] I.M. Gelfand and A.M. Yaglom, Calculation of the amount of information about a random function contained in another such function, Amer. Math. Soc. Transl., **12**, pp.199-246, 1959.

[26] H.Hasegawa, Dynamical formulation of quantum level ststistics, Open Systems and Information dynamics, **4**, pp.359-377, 1997.

[27] T.Hida, Complexity in white noise analysis, The second international conference on quantum information, Meijyou Univ. 1999.

[28] A.S. Holevo, Some estimates for the amount of information transmittable by a quantum communication channel (in Russian), Problemy Peredachi Informacii, **9**, pp.3-11, 1973.

[29] E.C. Holmes, L.Q.Zhang, P.Simmonds, C.A. Ludlam, and A.J. L.Brown, Convergent and divergent sequence evolution in the surface envelope glycoprotein of human immunodeficiency virus type 1 within a single infected patient, Evolution, **89**, pp.4835-4839, 1992.

[30] R.S. Ingarden, Quantum information theory, Rep. Math. Phys., **10**, pp.43-73, 1976.

[31] R.S.Ingarden, A.Kossakowski and M.Ohya, *Information Dynamics and Open Systems,* Kluwer Academic Publishers, 1997.

[32] K.Inoue, A.Kossakowski and M.Ohya, On quantum chaos in a spin system, SUT preprint.

[33] K. Inoue, M. Ohya and H. Suyari, Characterization of quantum teleportation processes by nonlinear quantum channel and quantum mutual entropy, Physica D, 120, pp.117-124, 1998.

[34] K.Inoue, M.Ohya and K.Sato, Application od chaos degree to some dynamical systems, Chaos, Solitons & Fractals, 11, 1377-1385, 2000.

[35] K.Inoue, M.Ohya and I.V.Volovich, On chaos of quantum Baker's transformation, in preparation.

[36] R. Jozsa and B. Schumacher, A new proof of the quantum noiseless coding theorem, J. Mod. Opt., **41**, pp.2343-2350, 1994.

[37] J.J.de Jong, J.Goudsmit, W.Keulen, B.Klaver, W.Krone, M.Tersmette, and A.de Ronde, Human immunodeficiency virus type 1 clones chimeric for the envelope V3 domain differ in syncytium formation and replication capacity, Journal of Virology, **66**, pp.757-765, 1992.

[38] A.N. Kolmogorov, Theory of transmission of information, Amer. Math. Soc. Translation, Ser.2, **33**, pp.291–321, 1963.

[39] A.Kossakowski, M.Ohya and N.Watanabe, Quantum dynamical entropy for completely positive operator, Infinite Dimensional Analysis, Quantum Probability and Related Topics, 2, No.2, 267-282, 1999.

[40] T.Matsuoka and M.Ohya, Fractal dimensions of states and its application to Ising model, Reports on Mathematical Physics **36**, pp.365-379, 1995.

[41] L.B. Levitin, Physical information theory for 30 years: basic concepts and results, Springer Lect. Note in Phys., **378**, pp.101-110, 1991.

[42] G. Lindblad, Entropy, information and quantum measurements, Commun. Math. Phys., 33, pp.111-119, 1973.

[43] A.W. Majewski, Separable and entangled states of composite quantum systems; Rigorous description, Preprint.

[44] T.McNearney, Z.Hornickova, R.Markham, A.Birdwell, M.Arens, A.Saah, and L.Ratner, Relationship of human immunodeficiency virus type 1 sequence heterogeneity to stage of disease, Medical Sciences, **89**, pp.10247-10251, 1992.

[45] M.Misiurewicz, Absolutely continuous measutres for certain maps of interval, Publ. Math. IHES, **53**., pp.17-51, 1981.

[46] S.Miyazaki, H.Sugawara and M.Ohya, The efficiency of entropy evolution rate for construction of phylogenetic trees, Genes Genet. Syst., **71**, pp.323-327, 1996.

[47] N.Muraki and M.Ohya, Entropy functionals of Kolmogorov Sinai type and their limit theorems, Letters in Mathematical Physics, **36**, pp.327-335, 1996.

[48] N. Muraki, M. Ohya and D. Petz, Note on entropy of general quantum systems, Open Systems and Information Dynamics, **1**, No.1, pp.43–56, 1992.

[49] S.B.Needleman and C.D.Wunsch, A general method applicable to search for similarities in the amino acid sequence of two proteins, J.Mol.Biol., **48**, pp.443-453, 1970.

[50] J.von Neumann, Die Mathematischen Grundlagen der Quantenmechanik, Springer- Berlin, 1932.

[51] M.Ohya, Quantum ergodic channels in operator algebras, Journal of Mathematical Analysis and Applications, **84**, pp.318-327, 1981.

[52] M.Ohya, On compound state and mutual information in quantum information theory, IEEE Transaction of Information Theory, **29**, pp.770-774, 1983.

[53] M.Ohya, Note on quantum probability, Letter in Nuovo Cimento, **38**, pp.402-406, 1983.

[54] M.Ohya, Some aspects of quantum information theory and their applications to irreversible processes, Reports on Mathematical Physics, **27**, pp.19-47, 1989.

[55] M.Ohya, Information theoretical treatment of genes, The Trans. of The IEICE, **E 72, No.5,** pp. 556-560, 1989.

[56] M.Ohya, Information dynamics and its application to optical communication processes, Springer Lecture Notes in Physics, **378**, pp.81-92, 1991.

[57] M.Ohya, Fractal dimension of states, Quantum probability and Related Topics, **6**, pp.359-369, 1991.

[58] M.Ohya and S.Matsunaga, Coding and genes, Trans. IEICE-A, **J74**, No.7, pp.1075-1084, 1991.

[59] M.Ohya, S.Miyazaki and K.Ogata, On multiple alignment of genome sequences, IEICE Trans. Commun., **E75-B**, No.6, pp.453-457, 1992.

[60] M.Ohya and Y.Uesaka, Amino acid sequences and DP matching: A new method for alignment, Information Sciences, **63,** pp.139-151, 1992.

[61] M.Ohya, State change, complexity and fractal in quantum systems, Quantum Communications and Measurement, **2**, pp.309-320, 1995.

[62] M.Ohya, Entropy transmission in C*-dynamical systems, J.Math. Anal. Appl., 100, pp.222-235, 1984.

[63] M.Ohya, Fundamentals of quantum mutual entropy and capacity, Open Systems and Information Dynamics, 6, No.1, 69-78, 1999.

[64] M.Ohya, Complexity and fractal dimensions for quantum states, Open Systems and Information Dynamics, **4**, pp.141-157, 1997.

[65] M.Ohya, Applications of information dynamics to genome sequences, SUT preprint.

[66] M.Ohya, Complexities and their applications to characterization of chaos, International Journal of Theoretical Physics, **37**, No.1, pp495-505, 1998.

[67] M.Ohya, Foundation of entropy, complexity and fractal in quantum systems, International Congress of Probability toward 2000, pp.263-286.

[68] M.Ohya, *Mathematical Foundation of Quantum Computer,* Maruzen Publ. Company, 1999.

[69] M.Ohya and A.Masuda, NP problem in quantum algorithm, to appear in Open Systems and Information Dynamics.

[70] M.Ohya and D.Petz, *Quantum Entropy and Its Use,* Springer-Verlag, 1993.

[71] M. Ohya, D. Petz and N. Watanabe, On capacities of quantum channels, Prob. and Math. Phys., **17**, pp.179-196, 1997.

[72] M. Ohya, D. Petz and N. Watanabe, Numerical computation of quantum capacity, International J. Theor. Phys.,37, pp.507-510, 1998.

[73] M. Ohya and N. Watanabe, On mathematical treatment of Fredkin-Toffoli-Milburn gate, Physica D, 120, 206-213, 1998.

[74] C.H.Papadimitriou, *Computational Complexity*, Addison-Wisely, 1995.

[75] K.Sato, S.Miyazaki and M.Ohya, Analysis of HIV by entropy evolution rate, Amino Acids, **14**, pp.343-352, 1998.

[76] B. Schumacher, Sending entanglement through noisy quantum channels, Phy. Rev. A, **51**, pp.2614-2628, 1993.

[77] B. Schumacher, Quantum coding, Phy. Rev. A, 51, pp.2738-2747, 1993.

[78] P.H.Sellers, On the theory and computation of evolutionary distance, SIAM J. Appl. Math., **26**, No.4, pp.787-793, 1974.

[79] R.Shaw, Strange attractors, chaotic behavior and information flow, Z. Naturforsch, **36.a**, pp.80-112, 1981.

[80] C.E.Shannon, Mathematical theory of communication, Bell System Tech. J. 27, pp.379–423, 1948.

[81] P.W. Shor, Algorithm for quantum computation : Discrete logarithm and factoring algorithm, Proceedings of the 35th Annual IEEE Symposium on Foundation of Computer Science, pp.124-134, 1994.

[82] T.F.Smith, The genetic code, information density and evolution, Math. Biosci., **4**, pp.179-187, 1969.

[83] H.Tachibana, K.Sato and M.Ohya, On code structure of HIV, to be published.

[84] M.Toda, Crisis in chaotic scattering of a highly excited van der Waals complex, Physical Review Letters, **74**, No.14, pp.2670-2673, 1995.

[85] A.Uhlmann, Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in interpolation theory, Communication in Mathematical Physics, **54**, pp.21-32, 1977.

[86] H.Umegaki, Conditional expectations in an operator algebra IV (entropy and information), Kodai Math. Seminar Reports, **14**, pp.59-85, 1962.

[87] Voiculescu, D.,Commun. Math. Phys., 170, pp249-281, 1995.

[88] T.W.Wolfs, G.Zwart, M.Bakker, M.Valk,C.Kuiken, and J.Goudsmit, Naturally occurring mutations within HIV-1 V3 genomic RNA lead to antigenic variation dependent on a single amino acid substitution, Virology **185**, pp.195-205, 1991.

[89] H.P. Yuen and M. Ozawa, Ultimate information carrying limit of quantum systems, Phys. Rev. Lett., **70**, pp.363-366, 1993.