Asymptotic Attainment for Quantum Relative Entropy

Masahito Hayashi
Department of Mathematics, Kyoto University, Kyoto 606-01, Japan
e-mail address: masahito@kusm.kyoto-u.ac.jp

Abstract

In this paper it was proved that the quantum relative entropy $D(\sigma\|\rho)$ can be asymptotically attained by Kullback Leibler divergences of probabilities given by a certain sequence of measurements. The sequence of measurements depends on ρ, but is independent of the choice of σ.

In classical statistical theory the relative entropy $D(p\|q)$ is an information quantity which means the statistical efficiency in order to distinguish a probability measure p of a measurable space from another probability measure q of the same measurable space. The states correspond to measures on measurable space. When p, q are discrete probabilities, the relative entropy (called also information divergence) introduced by Kullback and Leibler is defined by [1]:

$$D(p\|q) := \sum_i p_i \log \frac{p_i}{q_i}.$$

In general, when p, q are measures on measurable space Ω, the relative entropy is defined by:

$$D(p\|q) := \int_\Omega \log \frac{dp}{dq}(\omega) p(\, d\omega),$$

where $\frac{dp}{dq}(\omega)$ is Radon-Nikodym derivative of p with respect to q.

Let $\mathcal{H}$ be a separable Hilbert space which corresponds to the physical system of interest. In quantum theory the relative entropy was first studied by Umegaki [2]. In quantum theory the states of a system corresponds to positive operators of trace one on $\mathcal{H}$. (These operators are called densities.) The quantum relative entropy of a states ρ with respect to another states σ is defined by:

$$D(\sigma\|\rho) := \mathrm{tr}\, \sigma(\log \sigma - \log \rho).$$

States are distinguished through the result of a quantum measurement on the system. The most general description of a quantum measurement probability is given by the mathematical concept of a *positive operator valued measure* (POM) [4,5] on the system state space. Generally speaking, if Ω is measurable space, a measurement M satisfies the following:

$$M(B) = M(B)^*, M(B) \geq 0, M(\emptyset) = 0, M(\Omega) = \mathrm{Id} \text{ on } \mathcal{H}, \text{ for any } B \subset \Omega.$$
$$M(\cup_i B_i) = \sum_i M(B_i), \text{ for } B_i \cap B_j = (i \neq j), \{B_i\} \text{ is countable subsets of } \Omega.$$

A measurement M on $\mathcal{H}$ is called *simple*, if for any $B \subset \Omega$, $M(B)$ is projection. In this paper, we treat only measurements whose measurable set is a finite set.

Let $\mathrm{tr}\, M(\cdot)\rho$ be the probability by a measurement M on a quantum system $\mathcal{H}$ with respect to a state ρ, then an information quantity we can directly access by a measurement M is not $D(\sigma\|\rho)$ but $D_M(\sigma\|\rho)$, where $D_M(\sigma\|\rho)$ denotes $D(\mathrm{tr}\, M(\cdot)\sigma\|\, \mathrm{tr}\, M(\cdot)\rho)$. Because the map $\rho \mapsto \mathrm{tr}\, M(\cdot)\rho$ is the dual of a unipreserving completely positive map [3], by Uhlmann inequality [6] we have

$$D_M(\sigma\|\rho) \leq D(\sigma\|\rho). \tag{1}$$

The equality is attained by a certain measurement M when and only when $\rho\sigma = \sigma\rho$. See for instance [7, Theorem 1.5, Theorem 5.3].

Can the equality of the inequality (1) be asymptotically attained? In order to answer the question we define the quantum i.i.d. condition which is the quantum analogue of the independent and identically distribution condition.

If there exist n samples of the state ρ, the quantum state is described by $\rho^{(n)}$ defined by:

$$\rho^{(n)} := \underbrace{\rho \otimes \cdots \otimes \rho}_{n} \text{ on } \mathcal{H}^{(n)},$$

where the composite system $\mathcal{H}^{(n)}$ is defined as:

$$\mathcal{H}^{(n)} := \underbrace{\mathcal{H} \otimes \cdots \otimes \mathcal{H}}_{n}.$$

In this paper, we consider this condition called the quantum i.i.d. condition. $\mathcal{B}(\mathcal{H})$ denotes the set of bounded operators on $\mathcal{H}$, and $\mathcal{B}(\mathcal{H})^{(n)}$ denotes $\underbrace{\mathcal{B}(\mathcal{H}) \otimes \cdots \otimes \mathcal{B}(\mathcal{H})}_{n}$.

Hiai and Petz proved the following theorem [8,9].

Theorem 1 *Let ρ, σ be states on $\mathcal{H}$, then there exists a sequence $\{(l_n, M_n)\}$ of pairs of an integer and a measurement on $\mathcal{H}^{(l_n)}$ such that*

$$\frac{D_{M_n}(\sigma^{(l_n)}\|\rho^{(l_n)})}{l_n} \to D(\sigma\|\rho) \ \textit{as}\ n \to \infty. \tag{2}$$

It was proved that there exists a sequence $\{M_n\}$ of measurements satisfying (2), but such a sequence $\{M_n\}$ was not constituted in Ref. [8,9]. It was not answered whether or not such a sequence depends on a state σ. Can we choose a sequence $\{M_n\}$ of measurements satisfying (2) which is independent of σ? The answer is "Yes". The main theorem of this paper is the following theorem.

Theorem 2 *Let ρ be a state on $\mathcal{H}$, then there exists a sequence $\{(l_n, M_n)\}$ of pairs of an integer and a measurement on $\mathcal{H}^{(l_n)}$ such that*

$$\frac{D_{M_n}(\sigma^{(l_n)}\|\rho^{(l_n)})}{l_n} \to D(\sigma\|\rho) \ \textit{as}\ n \to \infty\ \forall\sigma. \tag{3}$$

In this section we consider the relation between a simple measurement and a quantum relative entropy.

We put some definitions for this purpose. A state ρ is called *commutative* with a simple measurement $E(:=\{E_i\})$ on $\mathcal{H}$ if $[\rho, E_i] = 0$ for any i. For simple measurements E, F, we denote $E \leq F$ if for any i there exist subsets $\{A_i\}_i$ such that $E_i = \sum_{j\in A_i} F_j$. For a state ρ, E_ρ denotes the spectral decomposition of ρ. The *conditional expectation* $\mathcal{E}_E$ with respect to a simple measurement E is defined as:

$$\mathcal{E}_E : \rho \mapsto \sum_i E_i \rho E_i.$$

Theorem 3 *Let E be a simple measurement such that $w(E) := \sup_i \dim E_i < \infty$. If states ρ, σ are commutative with a simple measurement E and a simple measurement F satisfies that $E, E_\rho \leq F$, then we have*

$$D_F(\sigma\|\rho) \leq D(\sigma\|\rho) \leq D_F(\sigma\|\rho) + \log w(E).$$

Note that there exists a simple measurement F such that $E, E_\rho \leq F$.

Proof It is proved by Lemma 1 and Lemma 2. □

Lemma 1 *Let σ, ρ be states. If a simple measurement F satisfies that $E_\rho \leq F$, then*

$$D(\sigma\|\rho) = D_F(\sigma\|\rho) + D(\sigma\|\mathcal{E}_F(\sigma)). \tag{4}$$

Proof Since $E_\rho \leq F$, F is commutative with ρ. Thus we obtain (4) [7]. □

Lemma 2 *Let E, F be simple measurements such that $E \leq F$. If a state σ is commutative with E, then*

$$D(\sigma\|\mathcal{E}_F(\sigma)) \leq \log w(E). \tag{5}$$

Proof Let $a_i := \operatorname{tr} E_i\sigma E_i, \sigma_i := \frac{1}{a_i} E_i\sigma E_i$, then $\sigma = \sum_i a_i\sigma_i$. Therefore, from joint convexity of quantum relative entropy (See p.20 of [7]),

$$D(\sigma\|\mathcal{E}_F(\sigma)) \leq \sum_i a_i D(\sigma_i\|\mathcal{E}_F(\sigma_i)) \leq \sup_i D(\sigma_i\|\mathcal{E}_F(\sigma_i)) \leq \sup_i \log\dim E_i = \log w(E). \tag{6}$$

□

From the direct sum decomposition $\mathcal{H} = \mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_k$, we can naturally constitute the simple measurement $\{P_{\mathcal{H}_i}\}$, where $P_{\mathcal{H}_i}$ denotes the projection of $\mathcal{H}_i$. When $\mathcal{H}$ is finite-dimensional, we denote $Ir^{(n)}$ the simple measurement corresponding to a direct sum decomposition by the irreducible decomposition of the sensor space $\mathcal{H}^{(n)}$ of the act of $\mathrm{GL}(\mathcal{H})$.

Lemma 3 *If $\mathcal{H}$ is finite-dimensional, $Ir^{(n)}$ is commutative with $\sigma^{(n)}$ for any state σ.*

Proof If a state σ is faithful, then it is trivial by Schur's lemma. If a state σ isn't faithful, then there exists a sequence $\{\sigma_i\}$ of faithful states such that $\sigma_i \to \sigma$ as $i \to \infty$. Because $\sigma_i^{(n)} \to \sigma^{(n)}$ as $i \to \infty$ and $Ir^{(n)}$ is commutative with $\sigma_i^{(n)}$, $Ir^{(n)}$ is commutative with $\sigma^{(n)}$. □

Theorem 4 *Assume that the dimension of $\mathcal{H}$ is finite and is denoted by k. Let ρ be a state on $\mathcal{H}$. If a simple measurement M_n satisfies that $Ir^{(n)}, E_{\rho^{(n)}} \leq M_n$, then we obtain the following inequality:*

$$\frac{D_{M_n}(\sigma^{(n)}\|\rho^{(n)})}{n} \leq D(\sigma\|\rho) \leq \frac{D_{M_n}(\sigma^{(n)}\|\rho^{(n)})}{n} + (k-1)\frac{\log(n+1)}{n} \ \forall\sigma. \tag{7}$$

Therefore we obtain

$$\frac{D_{M_n}(\sigma^{(n)}\|\rho^{(n)})}{n} \to D(\sigma\|\rho) \ \textit{as}\ n \to \infty \ \textit{uniformally for}\ \sigma. \tag{8}$$

Proof Since $w(Ir^{(n)})$ is the dimension of the k-th symmetric tensor space of $\mathcal{H}$, $w(Ir^{(n)}) = {}_kH_n = \binom{n+k-1}{k-1} = \binom{n+k-1}{n} = {}_{n+1}H_{k-1} \leq (n+1)^{k-1}$, where ${}_kH_n$ denotes the repeated combination of n from k. Therefore, we have $\log w(Ir^{(n)}) \leq (k-1)\log(n+1)$. From Theorem 3 and Lemma 3 we have (7). □

Next we consider the infinite-dimensional case.

Theorem 5 *Let ρ be a state on $\mathcal{H}$, then there exists a sequence $\{(l_n, M_n)\}$ of pairs of an integer and a measurement on $\mathcal{H}^{(l_n)}$ such that*

$$\frac{D_{M_n}(\sigma^{(l_n)}\|\rho^{(l_n)})}{l_n} \to D(\sigma\|\rho) \ \textit{as}\ n \to \infty \ \forall\sigma. \tag{9}$$

Proof The finite-dimensional case is trivial from Theorem 4. We may assume that the dimension of $\mathcal{H}$ is infinite. Because of $\mathcal{B}(\mathcal{H})$'s injectivity, there exists a sequence $\{\alpha_n : \mathcal{B}(\mathcal{H}_n) \to \mathcal{B}(\mathcal{H})\}$ of unipreserving completely positive maps such that $\mathcal{H}_n$ is finite-dimensional and

$$\lim_{n\to\infty} D(\alpha_n^*(\sigma)\|\alpha_n^*(\rho)) = D(\sigma\|\rho) \tag{10}$$

for any normal states σ, ρ on $\mathcal{H}$ such that $\mu\rho \leq \sigma \leq \lambda\rho$ for some positive real numbers μ, λ [7]. From (8), for any positive integer n there exist a pair (l_n, M_n') of an integer and a simple measurement on $\mathcal{H}_n^{(l_n)}$ such that

$$D(\alpha_n^*(\sigma)\|\alpha_n^*(\rho)) - \frac{D_{M_n'}(\alpha_n^*(\sigma)^{(l_n)}\|\alpha_n^*(\rho)^{(l_n)})}{l_n} < \frac{1}{n}. \tag{11}$$

The completely positive map $\alpha_n^{(l)}$ from $\mathcal{B}(\mathcal{H}_n)^{(l)}$ to $\mathcal{B}(\mathcal{H})^{(l)}$ is defined as $\alpha_n^{(l)}(A_1 \otimes A_2 \otimes \cdots \otimes A_l) = \alpha_n(A_1) \otimes \alpha_n(A_2) \otimes \cdots \otimes \alpha_n(A_l)$ for $\forall A_i \in \mathcal{B}(\mathcal{H})$. Therefore we have $\alpha_n^{(l)*}(\sigma^{(l)}) = \alpha_n^*(\sigma)^{(l)}$. Let M_n be $\alpha_n^{(l_n)}(M_n')$, then from (10)(11) we get

$$\begin{aligned}
\frac{D_{M_n}(\sigma^{(l_n)}\|\rho^{(l_n)})}{l_n} &= \frac{D_{M_n'}\left(\alpha_n^{(l_n)*}\left(\sigma^{(l_n)}\right)\middle\|\, \alpha_n^{(l_n)*}\left(\rho^{(l_n)}\right)\right)}{l_n} \\
&= \frac{D_{M_n'}\left(\alpha_n^*(\sigma)^{(l_n)}\middle\|\, \alpha_n^*(\rho)^{(l_n)}\right)}{l_n} \\
&> D\left(\alpha_n^*(\sigma)\|\alpha_n^*(\rho)\right) + \frac{1}{n} \\
&\to D(\sigma\|\rho) \text{ as } n \to \infty.
\end{aligned}$$

Therefore, we obtain (9). □
Note that the simple measurement M_n is independent of σ. Therefore, we could constitute a sequence $\{M_n\}$ of measurements satisfying (3).

Remark 1 *Even if $\rho_\epsilon \to \rho$ as $\epsilon \to 0$ and M_n satisfies the assumption of Theorem 4, the following equation is not always established:*

$$\lim_{\epsilon\to 0}\lim_{n\to\infty}\frac{D_{M_n}(\rho_\epsilon^{(n)}\|\rho^{(n)})}{n\epsilon^2} = \lim_{n\to\infty}\lim_{\epsilon\to 0}\frac{D_{M_n}(\rho_\epsilon^{(n)}\|\rho^{(n)})}{n\epsilon^2}. \tag{12}$$

The left hand of (12) is a important value in quantum local detection, but the right hand of (12) is closely related to quantum estimation.

The following is an example of Remark 1.

Example 1 *Let the dimension k of $\mathcal{H}$ be 2. Let us define the Pauli matrices σ_1, σ_2 in the usual way:*

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

Assume that

$$\begin{aligned} \rho &= \frac{1}{2}(\mathrm{Id} + \alpha\sigma_1), \ 0 < \alpha < 1 \\ \rho_\epsilon &= \frac{1}{2}(\mathrm{Id} + \alpha(\cos\epsilon\sigma_1 + \sin\epsilon\sigma_2)). \end{aligned}$$

then

$$\begin{aligned} \lim_{\epsilon\to 0}\frac{D_{M_n}(\rho_\epsilon^{(n)}\|\rho^{(n)})}{\epsilon^2} &= 0 \\ \lim_{\epsilon\to 0}\lim_{n\to\infty}\frac{D_{M_n}(\rho_\epsilon^{(n)}\|\rho^{(n)})}{n\epsilon^2} &= \lim_{\epsilon\to 0}\frac{D(\rho_\epsilon\|\rho)}{\epsilon^2} = \frac{1}{4}\alpha\log\frac{1+\alpha}{1-\alpha} > 0, \end{aligned}$$

where a sequence of measurments $\{M_n\}$ satisfies the assumption of Theorem 4.

Conclusions It was proved that the quantum relative entropy $D(\sigma\|\rho)$ is attained by the sequence of Kullback-Leibler divergences given by a certain sequence of measurements which is independent of σ. This formula is thought to be important for the quantum asymptotic detection and the quantum asymptotic estimation. To know the quantum asymptotic estimation, see [10]. The realization of the sequence of measurements are left for future study.

Acknowledgments The author wishes to thank Prof. D. Petz for essential suggestions about the extension in the infinite-dimensional case. He wishes to thank Prof. A. Fujiwara and Dr. M. Ishii for several discussions on this topic.

References

[1] S. Kullback and R. A. Leibler, Ann. Math. Statist. **22**, 79-86 (1951).

[2] H. Umegaki, Kodai Math. Sem. Rep. **14**, 59 (1962).

[3] M. Ozawa, J. Math. Phys. **25**, 79 (1984).

[4] C. W. Helstrom, *Quantum Detection and Estimation Theory,* (Academic Press, New York, 1976).

[5] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory,* (North_Holland, Amsterdam, 1982).

[6] A. Uhlmann, Commun. Math. Phys. **54**, 21 (1977).

[7] M. Ohya and D. Petz, *Qunatum Entropy and Its Use* (Springer, Berlin, 1993).

[8] F. Hiai and D. Petz, Commun. Math. Phys. **143**, 99-114 (1991).

[9] D. Petz, J. Funct. Anal. **120**, 82-97 (1994).

[10] M. Hayashi, Kyoto-Math **97-09** (1997). LANL e-print quant-ph/9704041.