IOPscience iopscience.iop.org

Home Search Collections Journals About Contact us My IOPscience

Asymptotics of quantum relative entropy from a representation theoretical viewpoint

This article has been downloaded from IOPscience. Please scroll down to see the full text article.

2001 J. Phys. A: Math. Gen. 34 3413

(http://iopscience.iop.org/0305-4470/34/16/309)

View the table of contents for this issue, or go to the journal homepage for more

Download details:
IP Address: 171.66.16.95
The article was downloaded on 02/06/2010 at 08:56

Please note that terms and conditions apply.

INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **34** (2001) 3413–3419 www.iop.org/Journals/ja PII: S0305-4470(01)20570-8

Asymptotics of quantum relative entropy from a representation theoretical viewpoint

Masahito Hayashi

Laboratory for Mathematical Neuroscience, Brain Science Institute, RIKEN 2-1 Hirosawa, Wako, Saitama 351-0198, Japan

E-mail: masahito@brain.riken.go.jp

Received 23 December 2000

Abstract

In this paper it is proved that the quantum relative entropy $D(\rho\|\sigma)$ can be asymptotically attained by the relative entropy of probabilities given by a certain sequence of positive-operator-valued measures (POVMs). The sequence of POVMs depends on σ, but is independent of the choice of ρ.

PACS numbers: 0367, 0220, 0365B

1. Introduction

In classical statistical theory, the relative entropy $D(p\|q)$ is an information quantity which represents the statistical efficiency in distinguishing a probability measure p from another probability measure q. In the quantum mechanical case, states are described by density operators on a Hilbert space $\mathcal{H}$, which represents a physical system of interest. We can distinguish quantum states by data given through quantum measurements. A quantum measurement is described by a positive-operator-valued measure (POVM) $M = \{M_i\}_{i\in I}$, which is a partition of the unit into positive operators. A POVM $M = \{M_i\}_{i\in I}$ satisfying $M_i^2 = M_i$ for any index i is called a projection-valued measure (PVM); this plays an important role in this paper. When the quantum measurement corresponding to a POVM M is made on the system in a state ρ, the data obey the probability distribution $P_\rho^M(i) := \mathrm{Tr}\, M_i\rho$.

The quantum relative entropy $D(\rho\|\sigma) := \mathrm{Tr}\,\rho(\log\rho - \log\sigma)$ is known as a quantum analogue of the relative entropy. However, the information quantity, which is directly linked to statistical significance, is not the quantum relative entropy $D(\rho\|\sigma)$, but the relative entropy $D^M(\rho\|\sigma) := D(P_\rho^M\|P_\sigma^M)$. Concerning the relation between the two quantities $D(\rho\|\sigma)$ and $D^M(\rho\|\sigma)$, we have the following inequality from the monotonicity of the quantum relative entropy [1, 2]:

$$D^M(\rho\|\sigma) \leqslant D(\rho\|\sigma) \tag{1}$$

where the equality holds for some M if and only if $\rho\sigma = \sigma\rho$ (see Petz [6], proposition 1.16 in Ohya–Petz [5] and Fujiwara–Nagaoka [7]). As for the inequality (1), Hiai and Petz [3] proved that even if the states ρ and σ are not commutative with one another, the equality is attained in an asymptotic setting as described below. First, we introduce the quantum i.i.d. condition in order to treat an asymptotic setting. Suppose that n independent physical systems are given in the same state ρ, then the quantum state of the composite system is described by $\rho^{\otimes n}$, defined by

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

where the tensored space $\mathcal{H}^{\otimes n}$ is defined by

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

We call this condition the quantum i.i.d. condition, which is a quantum analogue of the independent-identical-distribution condition. Under the quantum i.i.d. condition, the equation

$$D(\rho^{\otimes n}\|\sigma^{\otimes n}) = nD(\rho\|\sigma)$$

holds. Hiai and Petz [3] proved the following theorem. (For the infinite-dimensional case, see Petz [4].)

Theorem 1. *Let k be the dimension of $\mathcal{H}$ and let σ and ρ_n be states on $\mathcal{H}$ and $\mathcal{H}^{\otimes n}$, respectively. Then there exists a POVM M^n on tensored space $\mathcal{H}^{\otimes n}$ such that*

$$\frac{1}{n}D(\rho_n\|\sigma^{\otimes n}) - \frac{(k-1)\log(n+1)}{n} \leqslant \frac{1}{n}D^{M^n}(\rho_n\|\sigma^{\otimes n}) \leqslant \frac{1}{n}D(\rho_n\|\sigma^{\otimes n}). \quad (2)$$

When the limit $\lim_{n\to\infty}\frac{1}{n}D(\rho_n\|\sigma^{\otimes n})$ converges, the equation

$$\lim_{n\to\infty}\frac{1}{n}D^{M^n}(\rho_n\|\sigma^{\otimes n}) = \lim_{n\to\infty}\frac{1}{n}D(\rho_n\|\sigma^{\otimes n})$$

holds.

Theorem 1 tells us that there exists a sequence $\{M_n\}$ satisfying (2) which may depend on both $\{\rho_n\}$ and σ. In this paper, using a representation theoretical argument on the representation of $SL(\mathcal{H})$ on $\mathcal{H}^{\otimes n}$, we prove that there exists a sequence $\{M_n\}$ satisfying (2) which depends only on σ when the sequence $\{\rho_n\}$ satisfies the quantum i.i.d. condition; i.e. the state ρ_n is $\rho^{\otimes n}$. The following is the main theorem.

Theorem 2. *Let k be the dimension of $\mathcal{H}$ and let σ be a state on $\mathcal{H}$. Then there exists a POVM M^n on the tensored space $\mathcal{H}^{\otimes n}$ which satisfies*

$$D(\rho\|\sigma) - \frac{(k-1)\log(n+1)}{n} \leqslant \frac{1}{n}D^{M^n}(\rho^{\otimes n}\|\sigma^{\otimes n}) \leqslant D(\rho\|\sigma) \qquad \forall\rho. \quad (3)$$

In section 2, we prove theorem 2 and discuss the difference between our proof and the proof of theorem 1 given by Hiai and Petz [3]. In section 3, we explain some results in representation theory which are necessary for the proof of theorem 2. At the end of section 3, we construct the POVM M^n satisfying (3). In section 4, we extend theorem 2 to the infinite-dimensional case.

If we perform the POVM M^n satisfying (3), we can attain the quantum relative entropy $D(\rho\|\sigma)$ w.r.t. the rate of the second error probability in the quantum hypothesis testing: the null hypothesis is $\rho^{\otimes n}$ and the alternative is $\sigma^{\otimes n}$. Theorem 2 claims that the POVM M^n is independent of the alternative ρ. Therefore, the POVM M^n is useful for the quantum hypothesis testing, in which the alternative hypothesis consists of plural tensored states. In addition, an application of theorem 2 to the quantum estimation will be discussed in another paper [9] in preparation.

2. Proof of the main theorem

In this section, we will prove the main theorem after some discussions about PVMs and the quantum relative entropy in the non-asymptotic setting. We make some definitions for this purpose. A state ρ is called *commutative* with a PVM $E(=\{E_i\})$ on $\mathcal{H}$ if $\rho E_i = E_i \rho$ for any index i. For PVMs $E(=\{E_i\}_{i\in I})$, $F(=\{F_j\}_{j\in J})$, the notation $E \leqslant F$ means that for any index $i \in I$ there exists a subset $(F/E)_i$ of the index set J such that $E_i = \sum_{j\in(F/E)_i} F_j$. For a state ρ, we denote $E(\rho)$ by the spectral measure of ρ, which can be regarded as a PVM. The map $\mathcal{E}_E$ with respect to a PVM E is defined as

$$\mathcal{E}_E : \rho \mapsto \sum_i E_i \rho E_i \tag{4}$$

which is an affine map from the set of states to itself. Note that the state $\mathcal{E}_E(\rho)$ is commutative with a PVM E. If a PVM $F = \{F_j\}$ is commutative with a PVM $E = \{E_i\}$, then we can define the PVM $F \times E = \{F_j E_i\}$, which satisfies that $F \times E \geqslant E$ and $F \times E \geqslant F$.

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

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

This theorem follows from lemma 2 and lemma 3 below. Using theorem 3 and the following lemma, we will prove the main theorem.

Lemma 1. *There exists a PVM E^n on $\mathcal{H}^{\otimes n}$ which is commutative with $\rho^{\otimes n}$ for any ρ and satisfies the relation $w(E^n) \leqslant (n+1)^{(k-1)}$.*

Lemma 1 is proved in the next section from a representation theoretical viewpoint. Now, let E^n be a PVM satisfying the condition given in lemma 1. Then there exists a PVM F^n such that $F^n \geqslant E^n \times E(\sigma^{\otimes n})$ and that $w(F^n) = 1$. Using theorem 3, we have the following.

$$\begin{aligned} D(\rho\|\sigma) - \frac{(k-1)\log(n+1)}{n} &\leqslant \frac{1}{n} D(\mathcal{E}_{F^n}(\rho^{\otimes n})\|\mathcal{E}_{F^n}(\sigma^{\otimes n})) \\ &\leqslant D(\rho\|\sigma) \qquad \forall \rho. \end{aligned} \tag{6}$$

Since the condition $w(F^n) = 1$ implies the equation $D(\mathcal{E}_{F^n}(\rho^{\otimes n})\|\mathcal{E}_{F^n}(\sigma^{\otimes n})) = D^{F^n}(\rho^{\otimes n}\|\sigma^{\otimes n})$, we obtain theorem 2.

Let us compare the above argument with that of Hiai and Petz [3]. We first note that the inequality $D^F(\rho\|\sigma) \leqslant D(\mathcal{E}_F(\rho)\|\mathcal{E}_F(\sigma))$ holds for any PVM, but the equality, in general, does not hold unless $w(F) = 1$. Instead of (6), Hiai and Petz proved the following:

$$\begin{aligned} \frac{1}{n} D(\rho_n\|\sigma^{\otimes n}) - \frac{(k-1)\log(n+1)}{n} &\leqslant \frac{1}{n} D(\mathcal{E}_{E(\sigma^{\otimes n})}(\rho^{\otimes n})\|\mathcal{E}_{E(\sigma^{\otimes n})}(\sigma^{\otimes n})) \\ &\leqslant \frac{1}{n} D(\rho_n\|\sigma^{\otimes n}). \end{aligned} \tag{7}$$

In the case when $\rho_n = \rho^{\otimes n}$, this is the same as (6) except that $E(\sigma^{\otimes n})$ is substituted for F^n. Since $w(E(\sigma^{\otimes n})) = 1$ does not hold, however, $D(\mathcal{E}_{E(\sigma^{\otimes n})}(\rho^{\otimes n})\|\mathcal{E}_{E(\sigma^{\otimes n})}(\sigma^{\otimes n}))$ cannot be replaced with $D^{E(\sigma^{\otimes n})}(\rho^{\otimes n}\|\sigma^{\otimes n})$ here. In other words, even though the PVM $E(\sigma^{\otimes n})$ does not depend on a state ρ, the inequality (7) does not imply the existence of a PVM M^n depending only on σ and satisfying (3) for all ρ. Indeed, the PVM M^n which was shown to satisfy (2) in [3] is not $E(\sigma^{\otimes n})$, but $E(\sigma^{\otimes n}) \times E(\mathcal{E}_{E(\sigma^{\otimes n})}(\rho_n))$, which depends on ρ_n in general. Therefore, the discussion of Hiai and Petz [3] does not imply theorem 2.

Now, we prove two lemmas used in a proof of theorem 3. The following lemma 2 is the same as lemma 3.1 of Hiai and Petz [3] and theorem 1.13 of Ohya and Petz [5]. However, lemma 2 is proved in the following because it plays a particularly important role in our proof of the main theorem.

Lemma 2. *Let ρ, σ be states. If a PVM F satisfies $E(\sigma) \leqslant F$, then*

$$D(\rho\|\sigma) = D(\mathcal{E}_F(\rho)\|\mathcal{E}_F(\sigma)) + D(\rho\|\mathcal{E}_F(\rho)). \tag{8}$$

Proof. As $E(\sigma) \leqslant F$ and F is commutative with σ, we have $\mathrm{Tr}\,\mathcal{E}_F(\rho)\log\mathcal{E}_F(\sigma) = \mathrm{Tr}\,\rho\log\sigma$. Since ρ is commutative with $\log\rho$, we have $\mathrm{Tr}\,\mathcal{E}_F(\rho)\log\rho = \mathrm{Tr}\,\rho\log\rho$. Therefore, we obtain the following:

$$\begin{aligned} D(\mathcal{E}_F(\rho)\|\mathcal{E}_F(\sigma)) - D(\rho\|\sigma) &= \mathrm{Tr}\,\mathcal{E}_F(\rho)(\log\mathcal{E}_F(\rho) - \log\mathcal{E}_F(\sigma)) - \mathrm{Tr}\,\rho(\log\rho - \log\sigma) \\ &= \mathrm{Tr}\,\mathcal{E}_F(\rho)(\log\mathcal{E}_F(\rho) - \log\rho). \end{aligned}$$

This proves (8). □

Lemma 3. *Let E, F be PVMs such that $E \leqslant F$. If a state ρ is commutative with E, then we have*

$$D(\rho\|\mathcal{E}_F(\rho)) \leqslant \log w(E). \tag{9}$$

Proof. Let $a_i := \mathrm{Tr}\,E_i\rho E_i$, $\rho_i := \frac{1}{a_i}E_i\rho E_i$. Then we have $\rho = \sum_i a_i\rho_i$, $\mathcal{E}_F(\rho) = \sum_i a_i\mathcal{E}_F(\rho_i)$ and $\sum_i a_i = 1$. Therefore,

$$\begin{aligned} D(\rho\|\mathcal{E}_F(\rho)) &= \sum_i \mathrm{Tr}\,E_i\rho(\log\rho - \log\mathcal{E}_F(\rho)) \\ &= \sum_i \mathrm{Tr}\,E_i\rho E_i(E_i\log\rho E_i - E_i\log\mathcal{E}_F(\rho)E_i) \\ &= \sum_i a_i D(\rho_i\|\mathcal{E}_F(\rho_i)) \leqslant \sup_i D(\rho_i\|\mathcal{E}_F(\rho_i)) \\ &= \sup_i (\mathrm{Tr}\,\rho_i\log\rho_i - \mathrm{Tr}\,\mathcal{E}_F(\rho_i)\log\mathcal{E}_F(\rho_i)) \\ &\leqslant -\sup_i \mathrm{Tr}\,\mathcal{E}_F(\rho_i)\log\mathcal{E}_F(\rho_i) \leqslant \sup_i \log\dim E_i = \log w(E). \end{aligned}$$

Thus, we obtain inequality (9). □

It is interesting to compare (9) with lemma 3.2 of Hiai and Petz [3], which was used to show (7); i.e.,

$$D(\rho\|\mathcal{E}_F(\rho)) \leqslant \log h(F)$$

where $h(F)$ denotes the number of indices $i \in I$ for the PVM $F = \{F_i\}_{i\in I}$.

3. Quantum i.i.d. condition from group theoretical viewpoint

In this section, we discuss the quantum i.i.d. condition from a group theoretical viewpoint for the purpose of lemma 1. In section 3.1, we consider the relation between irreducible representations and PVMs. In section 3.2, we discuss the quantum i.i.d. condition and PVMs from a theoretical viewpoint.

3.1. Group representation and its irreducible decomposition

Let V be a finite-dimensional vector space over the complex numbers $\mathbb{C}$. A map π from a group G to the generalized linear group of a vector space V is called a *representation* on V if the map π is a homomorphism, i.e. $\pi(g_1)\pi(g_2) = \pi(g_1 g_2),\ \forall g_1, g_2 \in G$. A subspace W of V is called *invariant* with respect to a representation π if the vector $\pi(g)w$ belongs to the subspace W for any vector $w \in W$ and any element $g \in G$. A representation π is called *irreducible* if there is no proper nonzero invariant subspace of V with respect to π. Let π_1 and π_2 be representations of a group G on V_1 and V_2, respectively. The *tensored* representation $\pi_1 \otimes \pi_2$ of G on $V_1 \otimes V_2$ is defined as $(\pi_1 \otimes \pi_2)(g) = \pi_1(g) \otimes \pi_2(g)$, and the *direct sum* representation $\pi_1 \oplus \pi_2$ of G on $V_1 \oplus V_2$ is also defined as $(\pi_1 \oplus \pi_2)(g) = \pi_1(g) \oplus \pi_2(g)$.

In the following, we treat a representation π of a group G on a finite-dimensional Hilbert space $\mathcal{H}$. The following facts are crucial in the later arguments. There exists an irreducible decomposition $\mathcal{H} = \mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_l$ such that the irreducible components are orthogonal to one another if for any element $g \in G$ there exists an element $g^* \in G$ such that $\pi(g)^* = \pi(g^*)$, where $\pi(g)^*$ denotes the adjoint of the linear map $\pi(g)$. We can regard the irreducible decomposition $\mathcal{H} = \mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_l$ as the PVM $\{P_{\mathcal{H}_i}\}_{i=1}^{l}$, where $P_{\mathcal{H}_i}$ denotes the projection to $\mathcal{H}_i$. If two representations π_1, π_2 satisfy the preceding condition, then the tensored representation $\pi_1 \otimes \pi_2$ also satisfies it. Note that, in general, an irreducible decomposition of a representation satisfying the preceding condition is not unique. In other words, we cannot uniquely define the PVM from such a representation.

3.2. Relation between the tensored representation and PVMs

Let the dimension of the Hilbert space $\mathcal{H}$ be k. Concerning the natural representation $\pi_{SL(\mathcal{H})}$ of the special linear group $SL(\mathcal{H})$ on $\mathcal{H}$, we consider its nth tensored representation $\pi_{SL(\mathcal{H})}^{\otimes n} := \underbrace{\pi_{SL(\mathcal{H})} \otimes \cdots \otimes \pi_{SL(\mathcal{H})}}_{n}$ on the tensored space $\mathcal{H}^{\otimes n}$. For any element $g \in SL(\mathcal{H})$, the relation $\pi_{SL(\mathcal{H})}(g)^* = \pi_{SL(\mathcal{H})}(g^*)$ holds, where the element $g^* \in SL(\mathcal{H})$ denotes the adjoint matrix of the matrix g. Consequently, there exists an irreducible decomposition of $\pi_{SL(\mathcal{H})}^{\otimes n}$ regarded as a PVM and we denote the set of such PVMs by $\mathrm{Ir}^{\otimes n}$.

From the Weyl dimension formula ((7.1.8) or (7.1.17) of Goodman and Wallch [8]), the nth symmetric tensored space is the maximum-dimensional space in the irreducible subspaces with respect to the nth tensored representation $\pi_{SL(\mathcal{H})}^{\otimes n}$. Its dimension is equal to the repeated combination ${}_kH_n$ evaluated by ${}_kH_n = \binom{n+k-1}{k-1} = \binom{n+k-1}{n} = {}_{n+1}H_{k-1} \leqslant (n+1)^{k-1}$. Thus, any element $E^n \in \mathrm{Ir}^{\otimes n}$ satisfies that

$$w(E^n) \leqslant (n+1)^{k-1}. \tag{10}$$

Lemma 4. *A PVM $E^n \in \mathrm{Ir}^{\otimes n}$ is commutative with the nth tensored state $\rho^{\otimes n}$ of any state ρ on $\mathcal{H}$.*

Proof. If $\det \rho \neq 0$, then this lemma is trivial from the fact that $\det(\rho)^{-1}\rho \in SL(\mathcal{H})$. If $\det \rho = 0$, there exists a sequence $\{\rho_i\}_{i=1}^{\infty}$ such that $\det \rho_i \neq 0$ and $\rho_i \to \rho$ as $i \to \infty$. We have $\rho_i^{\otimes n} \to \rho^{\otimes n}$ as $i \to \infty$. Because a PVM $E^n \in \mathrm{Ir}^{\otimes n}$ is commutative with $\rho_i^{\otimes n}$, it is also commutative with $\rho^{\otimes n}$. □

Now, we can see that lemma 1 follows from lemma 4 and (10).

From the above discussion, if the PVM M^n satisfies $w(M^n) = 1$ and $E(\sigma^{\otimes n}) \times E^n \leqslant M^n$ for some $E^n \in \mathrm{Ir}^{\otimes n}$, the inequality (3) holds. In many cases, the relation $w(E(\sigma^{\otimes n}) \times E^n) = 1$ holds. Therefore, in these cases, the PVM $E(\sigma^{\otimes n}) \times E^n$ satisfies (3). For example, if the eigenvalues of σ are rationally independent of each other, the relation holds for arbitrary n. Also, in the spin-1/2 system except $\sigma = \frac{1}{2}\mathrm{Id}$, the relation holds. In this case, the POVM $E(\sigma^{\otimes n}) \times E^n$ can be regarded as a simultaneous measurement of the total momentum and the momentum of the direction specified by σ.

4. Infinite-dimensional case

Next, we prove an infinite-dimensional version of theorem 2. Let $\mathcal{B}(\mathcal{H})$ be the set of bounded operators on $\mathcal{H}$, and $\mathcal{B}(\mathcal{H})^{\otimes n}$ be $\underbrace{\mathcal{B}(\mathcal{H}) \otimes \cdots \otimes \mathcal{B}(\mathcal{H})}_{n}$. According to [5], from the separability of $\mathcal{H}$, there exists a finite-dimensional approximation of $\mathcal{H}$, i.e. a sequence $\{\alpha_n : \mathcal{B}(\mathcal{H}_n) \to \mathcal{B}(\mathcal{H})\}$ of unit-preserving completely positive maps such that $\mathcal{H}_n$ is finite dimensional and

$$\lim_{n\to\infty} D(\alpha_n^*(\rho)\|\alpha_n^*(\sigma)) = D(\rho\|\sigma) \tag{11}$$

for any states ρ, σ on $\mathcal{H}$ such that $\mu\sigma \leqslant \rho \leqslant \lambda\sigma$ for some positive real numbers μ, λ, where α_n^* is the adjoint of α_n. From (3) and (11), for any positive integer n there exists a pair $(l_n, M^{n\prime} := \{M_i^{n\prime}\})$ of an integer and a PVM on $\mathcal{H}_n^{\otimes l_n}$ such that

$$D(\alpha_n^*(\rho)\|\alpha_n^*(\sigma)) - \frac{D^{M^{n\prime}}\left((\alpha_n^*(\rho))^{\otimes l_n} \,\|(\alpha_n^*(\sigma))^{\otimes l_n}\right)}{l_n} < \frac{1}{n}. \tag{12}$$

The completely positive map $\alpha_n^{\otimes l}$ from $\mathcal{B}(\mathcal{H}_n)^{\otimes l}$ to $\mathcal{B}(\mathcal{H})^{\otimes l}$ is defined as $\alpha_n^{\otimes l}(A_1 \otimes A_2 \otimes \cdots \otimes A_l) = \alpha_n(A_1) \otimes \alpha_n(A_2) \otimes \cdots \otimes \alpha_n(A_l)$ for $\forall A_i \in \mathcal{B}(\mathcal{H})$. We have $\left(\alpha_n^{\otimes l}\right)^* (\rho^{\otimes l}) = \alpha_n^*(\rho)^{\otimes l}$. Let $M^n := \{\alpha_n^{\otimes l_n}(M_i^{n\prime})\}$, then from (11), (12) we obtain

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

Therefore, we obtain an infinite-dimensional version of theorem 2. Note that such a POVM M^n is independent of ρ.

Conclusions

It is proved that the quantum relative entropy $D(\rho\|\sigma)$ is attained by the sequence of the relative entropies given by a certain sequence of PVMs which is independent of ρ. This formula is closely related to the quantum asymptotic detection. The physical realization of the sequence of measurements corresponding to PVMs satisfying (3) is left for future study. In the spin-1/2 system, it follows from the representation theoretical viewpoint in section 3 that it is enough to simultaneously measure the total momentum and the momentum of the direction specified by σ.

Acknowledgments

The author wishes to thank Professor H Nagaoka for encouragement and useful advice to complete this manuscript. He is also grateful to Professor D Petz for essential suggestions about the extension in the infinite-dimensional case. He is indebted to Professor A Fujiwara and Dr M Ishii for several discussions on this topic.

References

[1] Lindblad G 1975 *Commun. Math. Phys.* **40** 147
[2] Uhlmann A 1977 *Commun. Math. Phys.* **54** 21
[3] Hiai F and Petz D 1991 *Commun. Math. Phys.* **143** 99–114
[4] Petz D 1994 *J. Funct. Anal.* **120** 82–97
[5] Ohya M and Petz D 1993 *Quantum Entropy and Its Use* (Berlin: Springer)
[6] Petz D 1985 Properties of quantum entropies *Quantum Probability and Application II (Lecture Notes in Mathematics vol 1136)* ed L Accardi and W von Waldenfels (Berlin: Springer) pp 428–41
[7] Fujiwara A and Nagaoka H 1998 *IEEE* **44** 1071–86
[8] Goodman R and Wallch N 1998 *Representations and Invariants of the Classical Groups* (Cambridge: Cambridge University Press)
[9] Hayashi M and Nagaoka H in preparation