The 24th Symposium on Information Theory
and Its Applications (SITA2001)
Kobe, Hyogo, Japan, Dec. 4 - 7, 2001

一般量子情報源における量子仮説検定
Quantum hypothesis testing for the general quantum hypotheses

林 正人*
Masahito Hayashi

Abstract—We discuss an asymptotic theory for quantum hypothesis testing of the general quantum hypotheses. As a corollary, we obtain a better evaluation of the exponent of the correct probability of hypothesis testing than Ogawa-Nagaoka's result.

Keywords—Information spectrum, Quantum Hypothesis testing, Exponent of correct probability, Quantum Stein's lemma, General quantum hypotheses

1 はじめに

量子系での単純た仮説検定問題は非漸近的な場合は Helstrom により, 量子 Neymann-Pearson の補題が得られ, さらに, Hiai-Petz, Ogawa-Nagaoka により, 漸近的な場合を扱う Stein の補題の量子版が得られた. 本稿では, より一般的な情報源に対して, 仮説検定問題を扱い, その帰結として, 量子版 Stein の補題や, 仮説検定の強逆指数を表す, Han-Kobayashi の補題の量子版を議論する. そして, Ogawa-Nagaoka により得られた強逆指数の評価より tight な評価を行う. 手法としては, 韓により, 展開されら情報スペクトル的手法のある種の量子版を考える. ただし, ここで扱った定式化以外に情報スペクトル的手法の量子版を考えることができる.

一般に対象となる量子の表現空間を Hilbert 空間 $\mathcal{H}$ とすると, その量子系での状態は $\mathcal{H}$ 上の密度演算子 ($\mathcal{H}$ 上の非負定値 かつ Trace が 1 となる自己共役作用素) で記述される.(密度演算子の集合を $\mathcal{S}(\mathcal{H})$ で表すことにする.) そしてその量子系での測定は $\mathcal{H}$ 上の非負定値作用素による単位の分解 $\{M_i | \sum_{i=1}^k M_i = \mathrm{I}\}$ で記述される. 以下ではこの単位の分解のことを測定と呼ぶことにする. (正作用素値測度 (Positive Operator Valued Measure) とも呼ばれ POVM と略されることもある.) そして, 状態 $\rho \in \mathcal{S}(\mathcal{H})$ を測定 $\{M_i | \sum_{i=1}^k M_i = \mathrm{I}\}$ で測定したとき測定値が従う確率分布 P_ρ^M は次で与えられる: $\mathrm{P}_\rho^M(i) := \mathrm{Tr}[M_i \rho]$.

今, 対象とする量子力学系の状態が ρ か σ のどちらかで表されると仮定し, 実際にどちらであるかを何らかの測定をもとに判断する仮説検定問題を考える. この場合, 測定結果として必要なのは ρ, σ どちらの状態を支持するかという 2 値であるから, $T_\rho + T_\sigma = I$ を満たす非負自己共役作用素のペア $\{T_\rho, T_\sigma\}$ で表される. さらに,$T_\rho = \mathrm{I} - T$,$T_\sigma = T$ とおくことにより, 任意の検定は $0 \le T \le I$ なる自己共役作用素 T によって表されることがわかる. このとき, 真の状態が ρ であるのに間違って σ であると判断してしまう確率 (第一種の誤り確率と呼ぶ) は $\alpha(T) := \mathrm{Tr}[\rho T_\sigma] = \mathrm{Tr}[\rho T]$, 逆に真の状態が σ であるのに ρ と判断してしまう確率 (第二種の誤り確率) は $\beta(T) := \mathrm{Tr}[\sigma T_\rho] = 1 - \mathrm{Tr}[\sigma T]$ となる. (T は ρ の受容域を表している.) 以下では長岡 [4, 5] にならって次のような一般的な漸近的状況を考える. 今, 状態を要素とする無限列 $\vec{\rho} = \{\rho_n\}$ および $\vec{\sigma} = \{\sigma_n\}$ が与えられたとする. ここで, 各 n に対し ρ_n と σ_n は共通のヒルベルト空間 $\mathcal{H}_n$ 上の密度作用素であるとするが, 異なる n に対する ρ_n, σ_n, $\mathcal{H}_n$ の間にはどんな関係も仮定しない. 本稿では検定の無限列 $\vec{T} = \{T_n\}$ (T_n は $0 \le T_n \le I$ を満たす $\mathcal{H}_n$ 上の自己共役作用素) に対し, 第一種誤り確率 $\alpha_n(T_n) := \mathrm{Tr}[\rho_n T_n]$ が 0 に近づくときの, 第二種誤り確率 $\beta_n(T_n) := 1 - \mathrm{Tr}[\sigma_n T_n]$ が 0 に近づく指数の限界を考える. その他, 第一種誤り確率 $\alpha_n(T_n)$ の 0 に近づく指数が r であるとき, r が十分大きいと, 第二種誤り確率 $\beta_n(T_n)$ は 1 に漸近する. この場合, 正しく検定される確率 $1 - \beta_n(T_n) = \mathrm{Tr}[\sigma_n T_n]$ の $n \to \infty$ における漸近的挙動に注目する.

後者の問題は一見無意味のように見えるが, 暗号の盗聴に対する安全性を問題にするとき意味があると思われる. 以下 §2 では古典論の結果をまとめ, §3 では量子系での一般的な場合での結果をまとめた. §4 では量子系での i.i.d. 条件に注目し, その条件の下での議論をまとめた. その結果,Ogawa-Nagaoka [1] によって得られた限界よりも, より強い限界を導出することができた. 最後に §5 では §3 で述べた主定理の 3 つ目の式を証明し, §6 では主定理の他の式の略証を与える.

2 古典論での仮説検定

ここで古典論の結果をまとめておく. 帰無仮説及び対立仮説がそれぞれ確率分布の列 $\vec{p} = \{p_n\}, \vec{q} = \{q_n\}$ で与えられているとする. なお, 第 1 種の誤り確率 $\alpha_n(T_n)$ 第 2 種の誤り確率 $\beta_n(T_n)$ については同じように定義することとする. すなわち $\alpha_n(T_n) := 1 - p_n(T_n), \beta_n(T_n) := q_n(T_n)$ とする. このとき, 以下の量を考える. 本稿では全ての極限は $n \to \infty$ を表すので $n \to \infty$ は省略した.

$$B(\epsilon|\vec{p}\|\vec{q}) := \sup_{\vec{T}} \left\{ \underline{\lim} \frac{-1}{n} \log \beta_n(T_n) \middle| \overline{\lim}\, \alpha_n(T_n) \le \epsilon \right\}$$

$$K(R|\vec{p}\|\vec{q}) := \overline{\lim}\, p_n \left\{ \frac{1}{n} \log \frac{p_n}{q_n} \le R \right\}$$

$$B^+(\vec{p}\|\vec{q}) := \inf_{\vec{T}} \left\{ \underline{\lim} \frac{-1}{n} \log \beta_n(T_n) \middle| \underline{\lim}\, \alpha_n(T_n) < 1 \right\}$$

$$K^+(R|\vec{p}\|\vec{q}) := \overline{\lim}\, p_n \left\{ \frac{1}{n} \log \frac{p_n}{q_n} > R \right\}$$

$$B_e^*(r|\vec{p}\|\vec{q}) :=$$
$$\inf_{\vec{T}} \left\{ \overline{\lim} \frac{-1}{n} \log(1 - \beta_n(T_n)) \middle| \underline{\lim} \frac{-1}{n} \log \alpha_n(T_n) \ge r \right\}$$

* 理化学研究所 脳科学総合研究センター 脳数理研究チーム〒 351-0198 埼玉県和光市広沢 2-1, Laboratory for Mathematical Meuroscience, Brain Science Institute, RIKEN. Wako, Saitama, 351-0198, JAPAN

$$\zeta^c\left(R|\vec{p}\|\vec{q}\right) := \overline{\lim}\frac{-1}{n}\log q_n\left\{\frac{1}{n}\log\frac{p_n}{q_n}\le R\right\}.$$

すなわち, 検定 $\vec{T}=(T_n)$ のうち第一種誤り確率が ϵ に漸近するようなものだけを考えるとき, 第二種誤り確率が 0 に近づく速さを表す指数 (rate) R ($\beta_n(T_n)\sim e^{-nR}$) をどこまで大きくできるか, その限界を表す量が $B(\epsilon|\vec{p}\,\|\,\vec{q})$ である. 一方第二種誤り確率が 0 に近づく指数 R を大きく取ると第一種誤り確率が漸近的に 1 になるが, その R についての限界を表す量が $B^+(\vec{p}\,\|\,\vec{q})$ である. さらに, 第一種誤り確率が 0 に近づく速さを表す指数 (rate)r を大きくしていき, $B^+(\vec{q}\,\|\,\vec{p})$ を超えると, 第二種誤り確率 β_n は漸近的に 1 に近づき, 正しく判定する確率 $1-\beta_n$ が 0 に漸近する. したがってその場合は $1-\beta_n$ が 0 に近づく指数 R をどれだけ小さくできるかが問題となり, その限界が $B_e^*(r|\vec{p}\,\|\,\vec{q})$ である.

これまでに知られている結果について以下に記す.

$$B(\epsilon|\vec{p}\,\|\,\vec{q}) = \sup\{R|K(R|\vec{p}\|\vec{q})\le\epsilon\} \quad (1)$$

$$B^+(\vec{p}\,\|\,\vec{q}) = \inf\{R|K^+(R|\vec{p}\|\vec{q})=0\} \quad (2)$$

$$B_e^*\left(r|\vec{p}\|\vec{q}\right) = \sup_R\min\{\zeta^c(R|\vec{p}\|\vec{q}), r+R\} \quad (3)$$

また, 第一種誤り確率が 0 に近づく速さを表す指数 (rate) が r 以上という条件の下で, 第二種誤り確率が 0 に近づく速さを表す指数 (rate) R の限界を表す量を問題にすることがある. この場合の古典版は知られているが, 今回の手法では量子版を解析することが出来なかったので, 触れないことにする.

特に p_n, q_n が確率分布 p, q の n 次の独立同一分布であるときには $0\le\epsilon<1$ となる ϵ について $B(\epsilon|\vec{p}\,\|\,\vec{q}) = D(p\|q) := \sum_i p_i\log\frac{p_i}{q_i}$ となることが Stein の補題として知られている.

3 量子系での仮説検定 (一般の場合)

本稿で導出する (3) の量子力学的対応物と Nagaoka-Hayashi[7] による (3) の量子力学的対応物はともに ρ_n と σ_n が可換である場合は (3) と一致する. まず各 E_i が射影となる測定 (PVM) $E=\{E_i\}_{i=1}^s$ について $w(E)$ を $w(E):=\sup_i \mathrm{rank}E_i$ で定義し, i の最大値 s を $h(E)$ で表す. 自己共役作用素 X と PVM $M=\{M_i\}$ について $XM_i=M_iX$ となるときこれらは互いに可換であると呼ぶ. 自己共役な Trace class 作用素 X, Y のスペクトル分解を $X:=\sum_i x_iE(X)_i, Y=\sum_j y_jE(Y)_j$ するとき, 状態 ρ に対して確率変数 $\overline{X},\overline{Y}$ に関する確率分布 $\mathrm{P}_\rho^{X,Y}$ を以下で定義する.

$$\mathrm{P}_\rho^{X,Y}(\overline{X}=x_i,\overline{Y}=y_j) := \mathrm{Tr}[E(X)_iE(Y)_j\rho E(Y)_j].$$

ここで定義した概念などを用いて次の量を定義する.

$$B(\epsilon|\vec{\rho}\,\|\,\vec{\sigma}) \stackrel{\mathrm{def}}{=} \sup_{\vec{T}}\left\{\underline{\lim}\frac{-1}{n}\log\beta_n(T_n)\middle|\overline{\lim}\,\alpha_n(T_n)\le\epsilon\right\}$$

$$K^{\vec{M}}(R|\vec{\rho}\|\vec{\sigma}) := K\left(R\middle|\left\{\mathrm{P}_{\rho_n}^{M^n}\right\}\middle\|\left\{\mathrm{P}_{\sigma_n}^{M^n}\right\}\right)$$

$$D^{\vec{M}}\left(\epsilon|\vec{\rho}\|\vec{\sigma}\right) := \sup\left\{R\middle|K^{\vec{M}}(R|\vec{\rho}\|\vec{\sigma})\le\epsilon\right\}$$

$$K(R|\vec{\rho}\|\vec{\sigma}) := \overline{\lim}\,\mathrm{P}_{\rho_n}^{\sigma_n,\rho_n}\left\{\frac{1}{n}\log\frac{\overline{\rho_n}}{\overline{\sigma_n}}\le R\right\}$$

$$D(\epsilon|\vec{\rho}\|\vec{\sigma}) := \sup\left\{R\,|K(R|\vec{\rho}\|\vec{\sigma})\le\epsilon\right\}$$

$$B^+(\vec{\rho}\,\|\,\vec{\sigma}) := \inf_{\vec{T}}\left\{\overline{\lim}\frac{-1}{n}\log\beta_n(T_n)\middle|\underline{\lim}\,\alpha_n(T_n)<1\right\}$$

$$K^{+,\vec{M}}(R|\vec{\rho}\|\vec{\sigma}) := K^+\left(R\middle|\left\{\mathrm{P}_{\rho_n}^{M^n}\right\}\middle\|\left\{\mathrm{P}_{\sigma_n}^{M^n}\right\}\right)$$

$$D^{+,\vec{M}}\left(\vec{\rho}\|\vec{\sigma}\right) := \inf\left\{R\middle|K^{\vec{M}}(R|\vec{\rho}\|\vec{\sigma})=0\right\}$$

$$K^+(R|\vec{\rho}\|\vec{\sigma}) := \overline{\lim}\,\mathrm{P}_{\rho_n}^{\sigma_n,\rho_n}\left\{\frac{1}{n}\log\frac{\overline{\rho_n}}{\overline{\sigma_n}}>R\right\}$$

$$D^+(\vec{\rho}\|\vec{\sigma}) := \inf\left\{R\,|K^+(R|\vec{\rho}\|\vec{\sigma})=0\right\}.$$

$$B_e^*\left(r|\vec{\rho}\|\vec{\sigma}\right) := \inf_{\vec{T}}\left\{\overline{\lim}\frac{-1}{n}\log(1-\beta_n(T_n))\middle|\underline{\lim}\frac{-1}{n}\log\alpha_n(T_n)\ge r\right\}$$

$$\zeta^c\left(R|\vec{\rho}\|\vec{\sigma}\right) := \overline{\lim}\frac{-1}{n}\log\mathrm{P}_{\sigma_n}^{\rho_n,\sigma_n}\left\{\frac{1}{n}\log\frac{\overline{\sigma_n}}{\overline{\rho_n}}\ge R\right\}$$

$$D_e^*(r|\vec{\rho}\|\vec{\sigma}) := \sup_R\min\{\zeta^c\left(R|\vec{\rho}\|\vec{\sigma}\right), r+R\}.$$

定理 1 状態の無限列 $\vec{\rho}=\{\rho_n\},\vec{\sigma}=\{\sigma_n\}$ に関して E^n が ρ_n,σ_n と可換とし, $\frac{\log w(E^n)}{n}\to 0$ となる PVM の無限列 $\vec{E}=\{E^n\}$ が存在するとき, 以下の式が成立する.

$$B(\epsilon|\vec{\rho}\|\vec{\sigma}) = \sup_{\vec{M}} D^{\vec{M}}\left(\epsilon|\vec{\rho}\|\vec{\sigma}\right) = D(\epsilon|\vec{\rho}\|\vec{\sigma}) = D^{\vec{M}_\sigma^E}\left(\epsilon|\vec{\rho}\|\vec{\sigma}\right). \quad (4)$$

$$B^+(\vec{\rho}\|\vec{\sigma}) = \sup_{\vec{M}} D^{+,\vec{M}}\left(\vec{\rho}\|\vec{\sigma}\right) = D^+(\vec{\rho}\|\vec{\sigma}) = D^{+,\vec{M}_\sigma^E}\left(\vec{\rho}\|\vec{\sigma}\right). \quad (5)$$

$$B_e^*\left(r|\vec{\rho}\|\vec{\sigma}\right) \ge D_e^*(r|\vec{\rho}\|\vec{\sigma}). \quad (6)$$

4 量子 i.i.d. 条件を満たす場合

以下 $\mathcal{H}_n=\mathcal{H}^{\otimes n}$ かつ $\mathcal{H}$ が有限次元の場合を考える. $\rho_n=\rho^{\otimes n}, \sigma_n=\sigma^{\otimes n}$ の場合は定理 1 の適用に必要な漸近的半可換性すなわち E^n が存在することについては文献 Hayashi[8] を見よ. この場合は確率分布 $\mathrm{P}_{\rho_n}^{\sigma_n,\rho_n}$ の下で確率変数 $\frac{1}{n}\log\overline{\rho_n}, \frac{1}{n}\log\overline{\sigma_n}$ がそれぞれ, $\mathrm{Tr}\,\rho\log\rho, \mathrm{Tr}\,\rho\log\sigma$ に確率収束することから, 量子 Stein の補題が導ける. さらに

$$\mathrm{E}_{\sigma^{\otimes n}}^{\rho^{\otimes n},\sigma^{\otimes n}}\left(\exp s\left(\log\frac{\overline{\sigma^{\otimes n}}}{\overline{\rho^{\otimes n}}}\right)\right) = \left(\mathrm{Tr}\,\sigma^{1+s}\rho^{-s}\right)^n$$

となることから, Gärtner-Ellis の定理 [10] を用いると以下を得る.

$$\zeta^c\left(R|\vec{\rho}\|\vec{\sigma}\right) = \sup_{s\ge0} sR - \log\mathrm{Tr}\,\sigma^{1+s}\rho^{-s}. \quad (7)$$

$R\le D(\sigma\|\rho)$ となるときは $\zeta\left(R|\vec{\rho}\|\vec{\sigma}\right)=0$ となる. さらに以下の定理を得る.

定理 2 $\rho_n=\rho^{\otimes n}, \sigma_n=\sigma^{\otimes n}, \mathcal{H}_n=\mathcal{H}^{\otimes n}$ かつ $\dim\mathcal{H}<\infty$ とする. 以下の式が成立する.

$$B_e^*\left(r|\vec{\rho}\|\vec{\sigma}\right) \ge \max_{s\ge0}\frac{sr-\log\mathrm{Tr}\,\sigma^{1+s}\rho^{-s}}{1+s}. \quad (8)$$

(8) に関連して Ogawa-Nagaoka[1] により不等式

$$B_e^*\left(r|\vec{\rho}\|\vec{\sigma}\right) \ge \max_{1\ge s\ge0}\frac{sr-\log\mathrm{Tr}\,\sigma^{1+s}\rho^{-s}}{1+s} \quad (9)$$

が示されている. 本稿の結果 (8) はわずかながら, (9) よりも優れた評価になっている. なお Ogawa-Nagaoka[1] においては $x \mapsto x^{-s}$ の作用素凸性 $(0 \le s \le 1)$ を用いたため, $s \ge -1$ という制限が付いてしまった. 本稿の手法では一切, 作用素単調性を用いていないので, そのような制限は無くなり, 上記のようなより強い主張が得られる. 参考までに古典系での i.i.d. の場合達成可能な限界は (8) である (Han-Kobayashi[11]).

定理 2 の証明: 以下,$B_e^*(r|\vec{\rho}\|\vec{\sigma}), \zeta^c(R|\vec{\rho}\|\vec{\sigma})$ をそれぞれ $B_e^*(r), \zeta^c(R)$ と書くことにする.

$\psi(s) := \log \mathrm{Tr}\, \sigma^{1+s}\rho^{-s}$ とおく. ψ の連続性及び (7) より, ζ^c の凸性及び連続性が言える. したがって $\zeta^c(R_*(r)) = r + R_*(r)$ を満たす $R_*(r)$ が一意に存在する. $D_e^*(r) = \sup_R \min\{\zeta^c(R), r+R\}$ であるから, (7) に注意すると $s \ge 0$ に対して, 以下の式を得る.

$$D_e^*(r) = \zeta^c(R_*(r)) \ge -sR_*(r) - \psi(s). \tag{10}$$

一方 $D_e^*(r) = r + R_*(r)$ より $R_*(r)$ を消去することにより

$$D_e^*(r) \ge \frac{sr - \psi(s)}{1+s}$$

を得る. よって (8) を得る. ■

5 (6) の証明

始めに以下の補題が成立する.

補題 3 状態 ρ, σ が $\mathrm{PVM}\ E$ と共に可換とする. このとき $0 \le T \le \mathrm{I}$ となる作用素 T 及び任意の実数 c に対して以下の不等式が成立する.

$$w(E)^{-1}\,\mathrm{Tr}\,\sigma T \le \mathrm{P}_\sigma^{\rho,\sigma}\{\overline{\sigma} \ge c\overline{\rho}\} + c\,\mathrm{Tr}\,\rho T. \tag{11}$$

(11) より以下の式が成立する.

$$\begin{aligned} & w(E_n)^{-1}(1-\beta_n(T_n)) \\ \le\ & \mathrm{P}_{\sigma_n}^{\rho_n,\sigma_n}\left\{\frac{1}{n}\log\frac{\overline{\rho_n}}{\overline{\sigma_n}} \le R\right\} + e^{-nR}\alpha_n(T_n). \end{aligned}$$

ここで $\underline{\lim}\frac{-1}{n}\log\alpha_n(T_n) \ge r$ とすると以下の不等式を得る.

$$\overline{\lim}\frac{-1}{n}\log(1-\beta_n(T_n)) \ge \min\{r+R, \zeta(R|\vec{\rho}\|\vec{\sigma})\}$$

したがって,

$$\overline{\lim}\frac{-1}{n}\log(1-\beta_n(T_n)) \ge D_e^*(r|\vec{\rho}\|\vec{\sigma})$$

を得る. すなわち,

$$B_e^*(r|\vec{\rho}\|\vec{\sigma}) \ge D_e^*(r|\vec{\rho}\|\vec{\sigma})$$

となり (6) を得る.

補題 3 の証明: $\sigma = \sum_i \sigma_i E(\sigma)_i, \rho = \sum_j \rho_j E(\rho)_j$ とスペクトル分解する. そして $D := \{(i,j)|\sigma_i \ge c\rho_i\}$ とすると,

$$\mathrm{P}_\sigma^{\rho,\sigma}\{\overline{\sigma} \ge c\overline{\rho}\} = \mathrm{Tr}\,\mathcal{E}^D(\sigma) \tag{12}$$

を得る. ただし, $\mathcal{E}^D(\sigma) := \sum_{(i,j)\in D} E(\rho)_j E(\sigma)_i \sigma E(\sigma)_i E(\rho)_j$ と定義した. これらの式と以下の補題 4 を用いると以下の式を得る. (最後の不等式で補題 4 を用いる.)

$$\begin{aligned} & \mathcal{E}^D(\sigma) + c\rho \\ =& \sum_{(i,j)\in D} \sigma_i E(\rho)_j E(\sigma)_i E(\rho)_j + \sum_j c\rho_j E(\rho)_j \\ =& \sum_{(i,j)\in D} \sigma_i E(\rho)_j E(\sigma)_i E(\rho)_j + \sum_{(i,j)\in D} c\rho_j E(\rho)_j E(\sigma)_i E(\rho)_j \\ & + \sum_{(i,j)\in D^c} c\rho_j E(\rho)_j E(\sigma)_i E(\rho)_j \\ \ge& \sum_{(i,j)\in D} \sigma_i E(\rho)_j E(\sigma)_i E(\rho)_j + \sum_{(i,j)\in D^c} \sigma_i E(\rho)_j E(\sigma)_i E(\rho)_j \\ =& \sum_{(i,j)} \sigma_i E(\rho)_j E(\sigma)_i E(\rho)_j = \mathcal{E}_{E(\rho)}(\sigma) \ge w(M)^{-1}\sigma. \end{aligned}$$

したがって $\mathcal{E}^D(\sigma) \ge w(M)^{-1}\sigma - c\rho$ を得る. これから

$$\begin{aligned} \mathrm{Tr}(w(M)^{-1}\sigma - c\rho)T &\le \mathrm{Tr}\,\mathcal{E}^D(\sigma)T \le \mathrm{Tr}\,\mathcal{E}^D(\sigma) \\ &= \mathrm{P}_\sigma^{\rho,\sigma}\{\overline{\sigma} \ge c\overline{\rho}\} \end{aligned}$$

となり (11) を得る. ■

補題 4 $\mathrm{PVM}\ M$ と状態 ρ がともに $\mathrm{PVM}\ E$ と可換であるとする. このとき

$$\mathcal{E}_M(\rho)w(E) \ge \rho \tag{13}$$

となる.

証明: $\dim\mathcal{H}$ の次元が k であるときに, $k\mathcal{E}_M(\rho) \ge \rho$ を示せば十分である. さらに ρ が純粋状態 $|\phi\rangle\langle\phi|$ のときに $\mathcal{E}_M(|\phi\rangle\langle\phi|)k \ge |\phi\rangle\langle\phi|$ を示せば十分である. 任意の $\psi \in \mathcal{H}$ に対して

$$\begin{aligned} & k\langle\psi|\mathcal{E}_M(|\phi\rangle\langle\phi|)|\psi\rangle - \langle\psi|\phi\rangle\langle\phi|\psi\rangle \\ =\ & k\sum_{i=1}^k \langle\psi|M_i|\phi\rangle\langle\phi|M_i|\psi\rangle - \left|\sum_{i=1}^k \langle\psi|M_i|\phi\rangle\right|^2 \ge 0 \end{aligned}$$

ここで最後の不等式は $\vec{a} = \{1\}_{i=1}^k$ というベクトルと $\vec{b} = \{\langle\psi|M_i|\phi\rangle\}_{i=1}^k$ というベクトルに関するシュワルツの不等式を適用すると導ける. よって (13) を得た. ■

6 (4) 及び (5) の証明の概略

古典系での結果 (1) から

$$B(\epsilon|\vec{\rho}\|\vec{\sigma}) = \sup_{\vec{M}} D^{\vec{M}}(\epsilon|\vec{\rho}\|\vec{\sigma})$$

が導ける. さらに以下の補題が成立する.

補題 5 ρ, σ が $\mathrm{PVM}\ E$ と可換とする.

$$\begin{aligned} & \inf\{\beta(T)\,|\alpha(T) \le \epsilon\} \\ &= \inf\left\{\beta(T)\ \middle|\ \begin{array}{c} \exists M : \mathrm{PVM}, \quad M \ge E, \\ M \ge E(T), \alpha(T) \le \epsilon, w(M) = 1 \end{array}\right\} \end{aligned}$$

となる.

証明: 任意の A に対して, $\beta(\mathcal{E}_E(T))=\beta(T), \alpha(\mathcal{E}_E(T))=\alpha(T)$ となる. PVM $E(\mathcal{E}_E(T))$ は E と可換であるから, $M\geq E, M\geq E(\mathcal{E}_E(T)), w(M)=1$ となる PVM M は存在する. ■

(4) を示すには以下の式 (14) を示すと十分であることが分かる.

$$\sup\left\{D^{\vec{M}}(\epsilon|\vec{\rho}\|\vec{\sigma}) \;\middle|\; \begin{array}{c} M^n\text{は}E^n\text{と可換で} \\ w(M^n)=1\text{となるPVM} \end{array}\right\}$$
$$= D^{\vec{M}^E_\sigma}(\epsilon|\vec{\rho}\|\vec{\sigma}) = D(\epsilon|\vec{\rho}\|\vec{\sigma}). \quad (14)$$

ここで以下の量を定義する.

$$\tilde{K}^{\vec{M}}(R|\vec{\rho}\|\vec{\sigma}) := \overline{\lim}\, \mathrm{P}_{\rho_n}^{\mathcal{E}_{M^n}(\sigma_n),\rho_n}\left\{\frac{1}{n}\log\frac{\overline{\rho_n}}{\overline{\mathcal{E}_{M^n}(\sigma_n)}}\leq R\right\}.$$

$K(R|\vec{\rho}\|\vec{\sigma})=\tilde{K}^{\vec{M}^E_\sigma}(R|\vec{\rho}\|\vec{\sigma})$ となることに注意せよ. (14) を示すために, 以下の 2 つの補題を用いる.

補題 6 状態 $\rho_n, {\sigma'}_n$ 及び PVM M^n はともに E^n と可換であり $\mathcal{E}_M({\sigma'}_n)={\sigma'}_n,\ w(M^n)=1,\ \frac{\log w(E^n)}{n}\to 0$ とする. このとき任意の実数 R 及び任意の $\delta>0$ について以下の式を得る.

$$\overline{\lim}\,\mathrm{P}_{\rho_n}^{{\sigma'}_n,\mathcal{E}_{M^n}(\rho_n)}\left\{\frac{1}{n}\log\frac{\overline{\mathcal{E}_{M^n}(\rho_n)}}{\overline{{\sigma'}_n}}\leq R-\delta\right\}$$
$$\leq \overline{\lim}\,\mathrm{P}_{\rho_n}^{{\sigma'}_n,\rho_n}\left\{\frac{1}{n}\log\frac{\overline{\rho_n}}{\overline{{\sigma'}_n}}\leq R\right\}$$
$$\leq \overline{\lim}\,\mathrm{P}_{\rho_n}^{{\sigma'}_n,\mathcal{E}_{M^n}(\rho_n)}\left\{\frac{1}{n}\log\frac{\overline{\mathcal{E}_{M^n}(\rho_n)}}{\overline{{\sigma'}_n}}\leq R+\delta\right\} \quad (15)$$

(15) に ${\sigma'}_n:=\mathcal{E}_{M^n}(\sigma_n)$ と代入し (21)(22) に注意すると任意の実数 R 及び任意の $\delta>0$ について以下の式を得る.

$$K^{\vec{M}}(R-\delta|\vec{\rho}\|\vec{\sigma})\leq\tilde{K}^{\vec{M}}(R|\vec{\rho}\|\vec{\sigma})\leq K^{\vec{M}}(R+\delta|\vec{\rho}\|\vec{\sigma}).$$

すなわち

$$\sup\left\{R\,\middle|\,K^{\vec{M}}(R|\vec{\rho}\|\vec{\sigma})\leq\epsilon\right\}=\sup\left\{R\,\middle|\,\tilde{K}^{\vec{M}}(R|\vec{\rho}\|\vec{\sigma})\leq\epsilon\right\}. \quad (16)$$

を得る.

補題 7 $\vec{M}=\{M^n\}$ を PVM の系列とする. さらに M_n 及び σ_n と可換な PVM E^n が取れて, $\frac{\log w(E^n)}{n}\to 0$ とする. このとき $\delta>0$ に対して以下の式が成立する.

$$K(R|\vec{\rho}\|\vec{\sigma})\leq\tilde{K}^{\vec{M}}(R+\delta|\vec{\rho}\|\vec{\sigma}). \quad (17)$$

したがって, 以下の式が成立する.

$$D(\epsilon|\vec{\rho}\|\vec{\sigma})\geq\sup\left\{R\,\middle|\,\tilde{K}^{\vec{M}}(R|\vec{\rho}\|\vec{\sigma})\leq\epsilon\right\}. \quad (18)$$

この 2 つの補題を用いて (14) を示す. 以下 M^n は E^n と可換で $w(M^n)=1$ を満たすとする. $\vec{M}:=\vec{M}^E_\sigma$ のときの補題 6 の (16) 及び $K(R|\vec{\rho}\|\vec{\sigma})=\tilde{K}^{\vec{M}^E_\sigma}(R|\vec{\rho}\|\vec{\sigma})$ となることに注意すると

$$D(\epsilon|\vec{\rho}\|\vec{\sigma})=D^{\vec{M}^E_\sigma}(\epsilon|\vec{\rho}\|\vec{\sigma}). \quad (19)$$

を得る. さらに補題 6 の (16) 及び補題 7 の (18) を組み合わせると以下を得る.

$$D^{\vec{M}}(\epsilon|\vec{\rho}\|\vec{\sigma})\leq D(\epsilon|\vec{\rho}\|\vec{\sigma}). \quad (20)$$

したがって (19) と (20) を組み合わせると (14) が得られる. 上の議論では以下の補題を用いた. 証明は容易である.

補題 8 $M\geq E(X), E(Y)$ となる PVM M について次の式が成立する.

$$\mathrm{P}_\rho^{X,Y}=\mathrm{P}_{\mathcal{E}_M(\rho)}^{X,Y}. \quad (21)$$

また σ と ρ が可換で, $\mathcal{E}_M(\rho)=\rho, \mathcal{E}_M(\sigma)=\sigma, w(M)=1$ となるときは以下の式が成立する.

$$\mathrm{P}_\rho^{\sigma,\rho}\left\{\log\frac{\overline{\rho}}{\overline{\sigma}}>a\right\}=\mathrm{P}_\rho^M\left\{\log\frac{\mathrm{P}_\rho^M}{\mathrm{P}_\sigma^M}>a\right\}. \quad (22)$$

したがって (4) の証明は補題 6 補題 7 に帰着できる. これらの証明は詳しくは文献 [14] を見よ. 同様にして,(5) を示すことができる.

References

[1] T. Ogawa and H. Nagaoka, "Strong Converse and Stein's Lemma in the Quantum Hypothesis Testing," LANL e-print quant-ph/9906090, (1999). IEEE Trans. Inform. Theory, vol. **IT**- 46, pp. 2428-2433 (2000).

[2] 小川 朋宏, 量子力学系における仮説検定と通信路符号化の漸近特性に関する研究, 電気通信大学大学院情報システム学研究科 学位申請論文, (2000).

[3] 韓 太舜, 「情報理論における情報スペクトル的方法」, 培風館, (1998).

[4] 長岡 浩司, 量子仮説検定の漸近論について, シンポジウム「統計的推測理論とその情報論的側面」予稿集, 49-52, (1998).

[5] 長岡 浩司, 量子仮説検定の情報スペクトル理論, 第２２回情報理論とその応用シンポジウム予稿集 245-247 (1999).

[6] 長岡 浩司, 量子仮説検定と大偏差:誤って検定される確率, 長岡メモ, June 17, (1999).

[7] H. Nagaoka and M. Hayashi, *IS Technical Reports,* UEC-IS-2000-5, 電気通信大学, (2000).

[8] M. Hayashi, "Asymptotics of Quantum Relative Entropy From Representation Theoretical Viewpoint," J. Phys. A: Math. and Gen. **34** 3413, (2001). LANL e-print quant-ph/9704040 (1997).

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

[10] A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications,* Jones and Bartlett Publishers, Boston, (1993).

[11] T. S. Han and K. Kobayashi, IEEE **IT 35**, 178-180, (1989).

[12] H. Nagaoka, Private communication, (2001).

[13] S. Osawa, Private communication, (2001).

[14] M. Hayashi, BSIS Technical Reports No.01-4 (2001). http://www.bsis.brain.riken.go.jp/BSIS-TR.html