数理解析研究所講究録
1534巻 2007年 109-118

量子通信路の漸近的可逆性

科学技術振興機構・さきがけ 小川 朋宏 (Tomohiro Ogawa)
PRESTO, Japan Science and Technology Agency

1 はじめに

量子通信路とはトレースを保存する完全正写像のことで，物理的には量子力学的ノイズや量子状態操作を一般的に記述する概念である．量子通信路を通して量子状態を忠実に伝送するための方法として，量子誤り訂正符号が知られている．これは量子計算で用いる量子状態をノイズから守るための研究として始まった [1] [2]．本稿では，量子誤り訂正符号の漸近理論として知られる量子状態伝送符号化定理 [3] [4] [5] について述べ，その一般化を試みる．

非漸近的な量子誤り訂正条件についての考察から，「量子状態を受信系に忠実に伝送すること」と「受信系以外の系 (環境系や盗聴者) に入力に関する情報を何も伝えないこと」が等価であることが分かる [6] [7]．Devetak はこの論法を漸近論において展開し，量子通信路において「盗聴から安全にメッセージを伝送すること」が実現されると「量子状態を忠実に伝送すること」が実現できること，「盗聴から安全にメッセージを伝送すること」は量子通信路 resolvability 問題に帰着されることを示した [4] .

量子通信路 resolvability 問題は，古典的情報理論における通信路 resolvability 問題 [8] の量子力学的拡張であり，[4] において暗に用いられてきた．林 [5] はこれを明確に意識し量子状態伝送符号化定理の情報スペクトル的証明を与えている．本稿のアプローチはこれに習っている．本稿では量子状態伝送符号化定理の review (2節) の後に次の結果を示す．

- 非漸近的な量子誤り訂正条件について，作用素環論の言葉で特徴付けを与える (3節).
- 量子通信路 resolvability 問題の一般公式に対する評価を与え (4節)，独立同一な量子通信路に限らない一般的な設定のもとで，量子状態伝送符号化容量の下限を与える (5節).

なお量子情報理論全般の教科書として [5] [9] を参照して頂きたい．

2 量子状態伝送符号化定理

$\mathcal{H}_A$, $\mathcal{H}_B$ を有限次元 Hilbert 空間とする．トレースを保存する完全正写像 (TP-CP 写像) $\mathcal{E}:\mathcal{L}(\mathcal{H}_A)\to\mathcal{L}(\mathcal{H}_B)$ は量子通信路 (quantum channel) または量子操作 (quantum operation) とよばれる．Hilbert 空間 $\mathcal{H}$ 上の量子状態とは，密度行列 $\rho\in\mathcal{S}(\mathcal{H}):=\{\rho\in\mathcal{L}(\mathcal{H})\,|\,\rho=\rho^*\geq 0,\mathrm{Tr}[\rho]=1\}$，または state $\varphi(\cdot)=\mathrm{Tr}[\rho\,\cdot\,]$ のことである．本稿では bracket 記法を用い，Hilbert 空間の内積 $\langle\xi,\eta\rangle$ では物理の慣習を用いる．すなわち，ξ に関して共役線形：$\langle c_1\xi_1+c_2\xi_2,\eta\rangle=c_1^*\langle\xi_1,\eta\rangle+c_2^*\langle\xi_2,\eta\rangle$，$\eta$ に関して線形であるとする．

量子通信路 $\mathcal{E}$ を n 回使用することで (すなわち，$\mathcal{E}^{\otimes n}:\mathcal{L}(\mathcal{H}_A^{\otimes n})\to\mathcal{L}(\mathcal{H}_B^{\otimes n})$ を使用することで)，できるだけ大きな次元をもつヒルベルト空間 $\mathcal{H}_n$ 上の任意の量子状態を "漸近的に忠実に" 伝送する方法 (符号化・復号化) の族を考える．これらの伝送方法についての "符号化レート" $\liminf_{n\to\infty}\frac{1}{n}\log\dim\mathcal{H}_n$ の上限を量子通信路 $\mathcal{E}$ の量子状態伝送容量とよび $C_q(\mathcal{E})$ と書く．このとき次の定理が成り立つ．

Proposition 1 (量子状態伝送符号化定理 [3] [4] [5])

$$C_q(\mathcal{E}) = \lim_{n\to\infty} \frac{1}{n} \max_{\rho_n \in \mathcal{S}(\mathcal{H}_A^{\otimes n})} I_c(\rho_n, \mathcal{E}^{\otimes n}) \tag{1}$$

ただし，$I_c(\cdot,\cdot)$ は coherent information [10] とよばれ，量子通信路 $\mathcal{E}: \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ と入力量子状態 $\rho_A \in \mathcal{S}(\mathcal{H}_A)$ について，以下で定義される量である．

任意の $\rho_A \in \mathcal{S}(\mathcal{H}_A)$ について，ある Hilbert 空間 $\mathcal{H}_R$ と純粋状態 $\rho_{RA} \in \mathcal{S}(\mathcal{H}_R \otimes \mathcal{H}_A)$ が存在して，部分トレースにより $\rho_A = \mathrm{Tr}_R[\rho_{RA}]$ とすることができる．このとき ρ_{RA} を purification，Hilbert 空間 $\mathcal{H}_R$ を参照系 (reference system) とよぶ．また $\mathrm{rank}\,\rho_{RA} = 1$ であるから，ある $|\Phi_{RA}\rangle \in \mathcal{H}_R \otimes \mathcal{H}_A$ により，$\rho_{RA} = |\Phi_{RA}\rangle\langle\Phi_{RA}|$ と書ける．この $|\Phi_{RA}\rangle$ を purification とよぶこともある．$\rho_{RB} = (\mathcal{I}_R \otimes \mathcal{E})(\rho_{RA})$ ($\mathcal{I}_R : \mathcal{L}(\mathcal{H}_R) \to \mathcal{L}(\mathcal{H}_R)$ は恒等写像)，$\rho_B = \mathrm{Tr}_R[\rho_{RB}]$ とおくと，coherent information は von Neumann エントロピー $H(\rho) := -\mathrm{Tr}[\rho \log \rho]$ を用いて次で定義される．

$$I_c(\rho_A, \mathcal{E}) := H(\rho_B) - H(\rho_{RB}) \tag{2}$$

$I_c(\rho_A, \mathcal{E})$ は ρ_A の purification の自由度によらないことが示される．

最後に「"漸近的に忠実に" 伝送」を正確に述べる．伝送したい量子状態 $\rho \in \mathcal{S}(\mathcal{H}_n)$ が与えられたとき，送信者は量子操作 $\mathcal{C}^n : \mathcal{S}(\mathcal{H}_n) \to \mathcal{S}(\mathcal{H}_A^{\otimes n})$ による符号化を行った後，$\mathcal{C}^n(\rho)$ を量子通信路 $\mathcal{E}^{\otimes n}$ に入力する．受信者は出力量子状態 $\mathcal{E}^{\otimes n}\mathcal{C}^n(\rho)$ から量子操作 $\mathcal{D}^n : \mathcal{S}(\mathcal{H}_B^{\otimes n}) \to \mathcal{S}(\mathcal{H}_n)$ により元の量子状態を復号する．符号 $(\mathcal{C}^n, \mathcal{D}^n)$ による量子状態伝送の誤りはトレースノルムを用いて次式で評価される．

$$\mathrm{Pe}(\mathcal{C}^n, \mathcal{D}^n) = \max_{\rho \in \mathcal{S}(\mathcal{H}_n)} \|\rho - \mathcal{D}^n \mathcal{E}^{\otimes n} \mathcal{C}^n(\rho)\|_1 \tag{3}$$

このとき量子状態伝送容量 $C_q(\mathcal{E})$ は $\lim_{n\to\infty} \mathrm{Pe}(\mathcal{C}^n, \mathcal{D}^n) = 0$ を満たす符号の列 $\{(\mathcal{C}^n, \mathcal{D}^n)\}_{n=1}^{\infty}$ についての符号化レート $\liminf_{n\to\infty} \frac{1}{n} \log \dim \mathcal{H}_n$ の上限として定義される．慣例として，量子状態伝送の誤りは忠実度 (fidelity) という量で定義されるが，トレースノルムで定義をしても漸近的に同等である．また，符号化については等距離作用素 $W : \mathcal{H}_n \to \mathcal{H}_A^{\otimes n}$ を用いた埋め込み $\mathcal{C}^n : \rho \in \mathcal{S}(\mathcal{H}_n) \mapsto W\rho W^* \in \mathcal{S}(\mathcal{H}_A^{\otimes n})$ の形に限っても十分であることが知られている [11]．

3 量子誤り訂正条件

本節では，非漸近的な状況で量子通信路への入力が完全に復元されるための条件 (完全量子誤り訂正条件) [12] [13] について，作用素環的特徴付けを与える．

量子通信路 $\mathcal{E}: \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ と量子状態族 $\mathcal{S} \subseteq \mathcal{S}(\mathcal{H}_A)$ について，逆向きの量子通信路 $\mathcal{R}: \mathcal{L}(\mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_A)$ が存在して $\forall \rho \in \mathcal{S}, \mathcal{R}\mathcal{E}(\rho) = \rho$ となるとき，$\mathcal{E}$ は量子状態族 $\mathcal{S}$ に関して可逆 (reversible) であるという．また，ある $\rho_0 \in \mathcal{S}(\mathcal{H}_B)$ が存在して $\forall \rho \in \mathcal{S}, \mathcal{E}(\rho) = \rho_0$ となるとき，$\mathcal{E}$ は量子状態族 $\mathcal{S}$ に関して消失的 (vanishing) であるという．特に量子誤り訂正符号の文脈においては，量子状態族 $\mathcal{S}$ として，ある部分空間 $\mathcal{K} \subseteq \mathcal{H}_A$ についての量子状態全体 $\mathcal{S}(\mathcal{K}) = \{\rho \in \mathcal{S}(\mathcal{H}_A) \,|\, \mathrm{support}(\rho) \subseteq \mathcal{K}\}$ を考える．また以下では，部分空間を対応する射影子 p により $p\mathcal{H}_A$ と表す．

TP-CP 写像 $\mathcal{E}: \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ について，ある Hilbert 空間 $\mathcal{H}_E$ と等距離作用素 $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ が存在して $\mathcal{E}(\rho) = \mathrm{Tr}_E[V\rho V^*]$ ($\rho \in \mathcal{S}(\mathcal{H}_A)$) と書ける (Stinespring-Kraus

表現). 等距離作用素 V は，$\mathcal{H}_E$ の ONS $\{|f_k\rangle\}_k$ と作用素の族 $E_k : \mathcal{H}_A \to \mathcal{H}_B$ により，

$$V = \sum_k E_k \otimes |f_k\rangle \ : \ |\psi\rangle \in \mathcal{H}_A \mapsto \sum_k E_k |\psi\rangle \otimes |f_k\rangle \in \mathcal{H}_B \otimes \mathcal{H}_E$$

と書け，$\{E_k\}_k$ は条件 $\sum_k E_k^* E_k = 1_A$ を満たす．これより $\mathcal{E}$ の operator sum 表現 $\mathcal{E}(\rho) = \sum_k E_k \rho E_k^*$ が導かれる．

TP-CP 写像 $\mathcal{E} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ に対して，dual $\mathcal{E}^* : \mathcal{L}(\mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_A)$ が $\mathrm{Tr}[\mathcal{E}(\rho)X] = \mathrm{Tr}[\rho\mathcal{E}^*(X)]$ $(\forall \rho \in \mathcal{S}(\mathcal{H}_A), \forall X \in \mathcal{L}(\mathcal{H}_B))$ で定義され unital CP 写像となる．$\mathcal{E}$ が上の Stinespring-Kraus 表現を持つとき，

$$\mathrm{Tr}[\mathcal{E}(\rho)X] = \mathrm{Tr}[\mathrm{Tr}_E[V\rho V^*]X] = \mathrm{Tr}[V\rho V^*(X \otimes 1_E)] = \mathrm{Tr}[\rho V^*(X \otimes 1_E)V]$$

より $\mathcal{E}^*(X) = V^*(X \otimes 1_E)V$ である．本来 Stinespring-Kraus 表現と言えばこちらを指すのであった．また，量子通信路 $\mathcal{F} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_E)$ を $\mathcal{F}(\rho) = \mathrm{Tr}_B[V\rho V^*]$ で定義する．このとき以下の定理が成り立つ．

Theorem 1 量子通信路 $\mathcal{E} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ について，Hilbert 空間 $\mathcal{H}_E$ と等距離作用素 $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ により Stinespring-Kraus 表現が与えられているとする．p を $\mathcal{H}_A$ 上の射影子とするとき，$\mathcal{E}$ の $\mathcal{S}(p\mathcal{H}_A)$ に関する可逆性について以下は同値である．ただし，$\mathcal{K} = \mathcal{H}_B \otimes \mathcal{H}_E$，$q = VpV^*$，$\mathcal{M} = \mathcal{L}(\mathcal{H}_B) \otimes 1_E$ とおき，$\mathcal{M} \vee \mathcal{N}$ は $(\mathcal{M} \cup \mathcal{N})''$ を表わすものとする．

(i) $(\{q\}' \wedge \mathcal{M})_q = \mathcal{L}(q\mathcal{K})$

(ii) $(\{q\} \vee \mathcal{M}')_q = \mathbb{C}q$

(iii) $q\mathcal{M}'q = \mathbb{C}q$

(iv) $pE_i^* E_j p \in \mathbb{C}p \quad (\forall i, j)$

(v) $\mathcal{E}$ は $\mathcal{S}(p\mathcal{H}_A)$ について可逆

(vi) $\mathcal{F}$ は $\mathcal{S}(p\mathcal{H}_A)$ について消失的

条件 (iv) と (v) の同値性は完全量子誤り訂正条件として知られている．以下をふまえると，作用素環の初等的な知識のもとで，上記の同値性は易しい．一般に unital CP 写像 $T : \mathcal{L}(\mathcal{H}_B) \to \mathcal{L}(\mathcal{H}_A)$ に対して，

$$\mathcal{A}_T = \{X \in \mathcal{L}(\mathcal{H}_B) \,|\, T(X^*)T(X) = T(X^*X), T(X)T(X^*) = T(XX^*)\}$$

は $*$-algebra で，multiplicative domain とよばれる．T の Steinspring-Kraus 表現を $T(X) = V^*(X \otimes 1_E)V = \sum_k E_k^* X E_k$ とすると，multiplicative domain は

$$\mathcal{A}_T = \left\{X \in \mathcal{L}(\mathcal{H}_B) \,\middle|\, X \otimes 1_E \in \{VV^*\}'\right\} = \{E_k E_l^* \,|\, k, l\}'$$

で与えられる [14]．条件 (i) での $\{q\}' \wedge \mathcal{M}$ は，$\mathcal{E}$ の $\mathcal{L}(p\mathcal{H}_A)$ への制限の dual $(\mathcal{E}|_{\mathcal{L}(p\mathcal{H}_A)})^*$ についての multiplicative domain である．また，この定理では有限次元の仮定は本質的ではなく，normal TP-CP 写像であればよい．以下に定理の証明を与える．

proof: (i) $\Leftrightarrow$ (ii) : $\mathcal{N} = \{q\} \vee \mathcal{M}'$ とおくと $\mathcal{N}' = \{q\}' \wedge \mathcal{M}$ で，$q \in \mathcal{N}$ より $(\mathcal{N}_q)' = (\mathcal{N}')_q$ が成立する．よって主張が成り立つ．

(ii)$\Leftrightarrow$(iii) : $q\mathcal{K}$への作用を考えることで$(\{q\}\vee\mathcal{M}')_q=(q\mathcal{M}'q)''$が分かる．これより主張が成り立つ．
(iii)$\Leftrightarrow$(iv) : Vpが$p\mathcal{H}_A$と$q\mathcal{K}$をつなぐ部分等距離作用素であるから，(iii)$\Leftrightarrow pV^*\mathcal{M}'Vp=\mathbb{C}p$である．$\mathcal{M}'=1_B\otimes\mathcal{L}(\mathcal{H}_E)$に注意すると，

$$\begin{aligned}pV^*\mathcal{M}'Vp&=\left\{\sum_{k,l}p(E_k^*\otimes\langle f_k|)(1_B\otimes Y)(E_l\otimes|f_l\rangle)p\;\middle|\;Y\in\mathcal{L}(\mathcal{H}_E)\right\}\\&=\left\{\sum_{k,l}c_{kl}\,pE_k^*E_lp\;\middle|\;c_{kl}\in\mathbb{C}\right\}\end{aligned}$$

となる．これより主張が成り立つ．
(i)$\Rightarrow$(v) : $\mathcal{N}=\{q\}\vee\mathcal{M}'$とおき，$\mathcal{Z}(\mathcal{N})$を$\mathcal{N}$のcenter，$z(q)\in\mathcal{Z}(\mathcal{N})$を$q$のcentral supportとする．$\mathcal{Z}(\mathcal{N})\subseteq\mathcal{N}'=\{q\}'\wedge\mathcal{M}\subseteq\mathcal{M}$に注意すると，$*$-同型写像

$$\mathcal{L}(p\mathcal{H}_A)\to\mathcal{L}(q\mathcal{K})=\mathcal{N}_q'\to\mathcal{N}_{z(q)}'\subseteq\mathcal{M}$$

により，写像$\pi:X\in\mathcal{L}(p\mathcal{H}_A)\to\pi(X)\otimes1_E\in\mathcal{M}$が定まる．特に$\pi$はCP写像である．定義より

$$\forall X\in\mathcal{L}(p\mathcal{H}_A),\,VXV^*=(\pi(X)\otimes1_E)q$$

であり，特に$q=(\pi(p)\otimes1_E)q$であるから，$((1-\pi(p))\otimes1_E)q=0$が成り立つ．ここでsupport projectionが$s(\varphi)=1-p$となる$\mathcal{L}(\mathcal{H}_A)$上の状態$\varphi$を用いて，$T:\mathcal{L}(\mathcal{H}_A)\to\mathcal{L}(\mathcal{H}_B)$を以下で定義する．

$$T(X)=\pi(pXp)+\varphi(X)(1-\pi(p))$$

Tはunital CP写像であり，$\forall\rho\in\mathcal{S}(p\mathcal{H}_A)$と$\forall X\in\mathcal{L}(\mathcal{H}_A)$に対して以下を満たす．

$$\begin{aligned}\mathrm{Tr}[\mathcal{E}(\rho)T(X)]&=\mathrm{Tr}[V\rho V^*(T(X)\otimes1_E)]\\&=\mathrm{Tr}[V\rho V^*(\pi(pXp)\otimes1_E)q]+\varphi(X)\,\mathrm{Tr}[V\rho V^*((1-\pi(p))\otimes1_E)q]\\&=\mathrm{Tr}[V\rho V^*VpXpV^*]\\&=\mathrm{Tr}[\rho X]\end{aligned}$$

すなわち，$\mathcal{R}=T^*$とおけば$\forall\rho\in\mathcal{S}(p\mathcal{H}_A)$, $\mathcal{R}\mathcal{E}(\rho)=\rho$である．
(v)$\Rightarrow$(i) : TP-CP写像$\mathcal{R}:\mathcal{L}(\mathcal{H}_B)\to\mathcal{L}(\mathcal{H}_A)$が存在して，$\forall\rho\in\mathcal{S}(p\mathcal{H}_A)$, $\mathcal{R}\mathcal{E}(\rho)=\rho$であるから，

$$\mathrm{Tr}[V\rho V^*VXV^*]=\mathrm{Tr}[\rho X]=\mathrm{Tr}[\mathcal{R}\mathcal{E}(\rho)X]=\mathrm{Tr}[\mathcal{E}(\rho)\mathcal{R}^*(X)]=\mathrm{Tr}[V\rho V^*(\mathcal{R}^*(X)\otimes1_E)]$$

が，$\forall\rho\in\mathcal{S}(p\mathcal{H}_A)$, $\forall X\in\mathcal{L}(\mathcal{H}_A)$について成り立つ．これより，特に$\forall X\in\mathcal{L}(p\mathcal{H}_A)$について

$$q(\mathcal{R}^*(X)\otimes1_E)q=qVXV^*q=VXV^*$$

である．不等式$\mathcal{R}^*(X^*)\mathcal{R}^*(X)\le\mathcal{R}^*(X^*X)$を用いると，

$$\begin{aligned}VX^*XV^*&=q(\mathcal{R}^*(X^*)\otimes1_E)q(\mathcal{R}^*(X)\otimes1_E)q\\&\le q(\mathcal{R}^*(X^*)\otimes1_E)(\mathcal{R}^*(X)\otimes1_E)q\\&\le q(\mathcal{R}^*(X^*X)\otimes1_E)q\\&=VX^*XV^*\end{aligned}$$

が成り立つ．よって，

$$\forall X \in \mathcal{L}(p\mathcal{H}_A),\ q(\mathcal{R}^*(X)\otimes 1_E)q = (\mathcal{R}^*(X)\otimes 1_E)q$$

が成立し，$\forall X \in \mathcal{L}(p\mathcal{H}_A)$ について $\mathcal{R}^*(X)\otimes 1_E$ と q は可換である．これより以下の包含関係が成り立つ．

$$\mathcal{L}(q\mathcal{K}) = V\mathcal{L}(p\mathcal{H}_A)V^* = (\mathcal{R}^*(\mathcal{L}(p\mathcal{H}_A))\otimes 1_E)q \subseteq (\{q\}'\wedge\mathcal{M})_q$$

逆向きの包含関係 $(\{q\}'\wedge\mathcal{M})_q \subseteq \mathcal{L}(q\mathcal{K})$ は明らかであるから主張が示された．
(iii) $\Leftrightarrow$ (vi) : (iii) を仮定すると $q(1_B\otimes\mathcal{L}(\mathcal{H}_E))q = \mathbb{C}q$ であるから，$\mathcal{L}(\mathcal{H}_E)$ 上の状態 φ_0 が存在して，

$$\forall Y \in \mathcal{L}(\mathcal{H}_E),\ q(1_B\otimes Y)q = \varphi_0(Y)q$$

である．よって $\forall\rho\in\mathcal{S}(p\mathcal{H}_A)$, $\forall Y\in\mathcal{L}(\mathcal{H}_E)$ に対して，

$$\mathrm{Tr}[\mathcal{F}(\rho)Y] = \mathrm{Tr}[V\rho V^*(1_B\otimes Y)] = \mathrm{Tr}[V\rho V^* q(1_B\otimes Y)q] = \varphi_0(Y)\,\mathrm{Tr}[V\rho V^* q] = \varphi_0(Y)$$

が成り立つ．すなわち $\mathcal{F}$ は消失的であり (vi) が導かれた．この論法を逆向きにたどることで (vi) $\Rightarrow$ (iii) が示される． □

4 量子通信路 resolvability 問題

量子通信路 resolvability 問題とは，量子通信路の出力が消失的になるように (出力から入力が全く分からないように)，入力側で意図的にランダマイズするときの必要な乱数のサイズを見積る問題である [8] [5].

ある集合 $\mathcal{X}$ から有限次元 Hilbert 空間 $\mathcal{H}$ 上の量子状態への写像 $F : x\in\mathcal{X}\mapsto\rho_x\in\mathcal{S}(\mathcal{H})$ と $\mathcal{X}$ 上の確率分布関数 $\{p(x)\}_{x\in\mathcal{X}}$ が与えられているとする．この写像 F は古典量子通信路ともよばれ，古典的メッセージを量子通信路を通して伝送するときの入出力関係が想定されている．この n 次独立同一拡大：

$$\begin{aligned} &F^n : x^n = (x_1, x_2, \ldots, x_n)\in\mathcal{X}^n \mapsto \rho_{x^n} = \rho_{x_1}\otimes\rho_{x_2}\otimes\cdots\otimes\rho_{x_n}\in\mathcal{S}(\mathcal{H}^{\otimes n}) \qquad (4)\\ &p^n(x^n) = p(x_1)p(x_2)\ldots p(x_n)\end{aligned}$$

を考え，アンサンブル平均を $\sigma_n = E_{p^n}[\rho_{x^n}]$ とおく．今の場合 $\sigma = E_p[\rho_x]$ とおけば $\sigma_n = \sigma^{\otimes n}$ である．ここで，$\mathcal{X}^n$ の部分集合 $\{x_1^n, x_2^n, \ldots, x_{L_n}^n\}\subseteq\mathcal{X}^n$ を上手に選ぶことにより，サンプル平均 $\frac{1}{L_n}\sum_{l=1}^{L_n}\rho_{x_l^n}$ とアンサンブル平均 σ_n が，漸近的に "区別ができない" ようにしたい．サンプル平均はサイズ L_n の一様乱数の出力を見て (サイコロを振って)，それに従って x_l^n を入力することで実現できる．このときの必要な乱数のサイズ L_n の限界を見積ることが量子通信路 resolvability 問題の目的で，L_n を $L_n\approx e^{nR}$ の形で増大さるとき，レート R をどこまで小さくできるかを問題にする．

以下では情報スペクトル的方法とよばれる一般的な状況のもとで議論をする．本来，情報スペクトル的方法において Hilbert 空間に有限次元の仮定を設けたくないのであるが，今のところ必要である．各 $n=1,2,\ldots$ に対して，集合 $\mathcal{X}^{(n)}$ から有限次元 Hilbert 空間 $\mathcal{H}^n$ 上の量子状態への写像 $F^n : x^n\in\mathcal{X}^{(n)}\mapsto\rho_{x^n}\in\mathcal{S}(\mathcal{H}^n)$ と，確率分布関数 $\{p^n(x^n)\}_{x^n\in\mathcal{X}^{(n)}}$ が与

えられているとし，これらの列を $\boldsymbol{F}=\{F^n\}_{n=1}^{\infty}, \boldsymbol{p}=\{p^n(\cdot)\}_{n=1}^{\infty}$ と書く．典型的には n 次独立同一拡大 (4) を想定していて，混乱のない限り $\mathcal{X}^{(n)}$ の括弧を省略して $\mathcal{X}^n$ と書くことにする．またアンサンブル平均を $\sigma_n=E_{p^n}[\rho_{x^n}]$ とおく．実数 R について，サイズ L_n の部分集合の列 $\{x_1^n,\ldots,x_{L_n}^n\}\subset\mathcal{X}^n$ $(n=1,2,\ldots)$ が存在して，

$$\limsup_{n\to\infty}\frac{1}{n}\log L_n\le R \tag{5}$$

$$\lim_{n\to\infty}\left\|\frac{1}{L_n}\sum_{l=1}^{L_n}\rho_{x_l^n}-\sigma_n\right\|_1=0 \tag{6}$$

を満たすとき，レート R は achievable であるという．量子通信路 resolvability 容量 $C_r(\boldsymbol{p},\boldsymbol{F})$ は achievable なレート R の下限として定義される．このように操作的に定義された resolvability 容量 $C_r(\boldsymbol{p},\boldsymbol{F})$ が，どのような情報量で書けるかが問題である．

エルミート作用素 A と $a\in\mathbb{R}$ に対して $\{A>a\}:=s((A-a)_+)$ (正部分へのサポート射影) とおく．ここで，Hilbert 空間 $\mathcal{H}^n$ を σ_n のサポートに限ることで，$\sigma_n>0$ を仮定しても一般性は失なわれない．resolvability 問題においては以下の情報量が重要である．

$$\underline{I}(\boldsymbol{p},\boldsymbol{F}):=\sup\left\{a\in\mathbb{R}\,\middle|\,\lim_{n\to\infty}E_{p^n}\operatorname{Tr}[\rho_{x^n}\{\rho_{x^n}-e^{na}\sigma_n>0\}]=1\right\} \tag{7}$$

$$\overline{I}(\boldsymbol{p},\boldsymbol{F}):=\inf\left\{a\in\mathbb{R}\,\middle|\,\lim_{n\to\infty}E_{p^n}\operatorname{Tr}[\rho_{x^n}\{\rho_{x^n}-e^{na}\sigma_n>0\}]=0\right\} \tag{8}$$

$$\underline{I}_{BS}(\boldsymbol{p},\boldsymbol{F}):=\sup\left\{a\in\mathbb{R}\,\middle|\,\lim_{n\to\infty}E_{p^n}\operatorname{Tr}\left[\rho_{x^n}\left\{\rho_{x^n}^{1/2}\sigma_n^{-1}\rho_{x^n}^{1/2}>e^{na}\right\}\right]=1\right\} \tag{9}$$

$$\overline{I}_{BS}(\boldsymbol{p},\boldsymbol{F}):=\inf\left\{a\in\mathbb{R}\,\middle|\,\lim_{n\to\infty}E_{p^n}\operatorname{Tr}\left[\rho_{x^n}\left\{\rho_{x^n}^{1/2}\sigma_n^{-1}\rho_{x^n}^{1/2}>e^{na}\right\}\right]=0\right\} \tag{10}$$

このとき次の定理が成り立つ．

Theorem 2 $R>\overline{I}_{BS}(\boldsymbol{p},\boldsymbol{F})$ ならば R は achievable である．すなわち，

$$\overline{I}_{BS}(\boldsymbol{p},\boldsymbol{F})\ge C_r(\boldsymbol{p},\boldsymbol{F}) \tag{11}$$

量子通信路 resolvability 容量についての一般公式は，まだ与えられていない．独立同一拡大 (4) における以下の考察により，残念ながら (11) の評価はタイトではないが，Hilbert 空間の有限次元性以外に何の仮定もおかない場合における評価という意義はある．

独立同一拡大 (4) では，(9) (10) について比較的容易に次式が示される．

$$\overline{I}_{BS}(\boldsymbol{p},\boldsymbol{F})=\underline{I}_{BS}(\boldsymbol{p},\boldsymbol{F})=I_{BS}(p):=E_p\operatorname{Tr}\left[\rho_x\log\left(\rho_x^{1/2}\sigma^{-1}\rho_x^{1/2}\right)\right] \tag{12}$$

一方で量子仮説検定の理論 [15] [16] [17] において，(7) (8) に関して次式が示されている．

$$\overline{I}(\boldsymbol{p},\boldsymbol{F})=\underline{I}(\boldsymbol{p},\boldsymbol{F})=I(p):=E_pD(\rho_x\|\sigma) \tag{13}$$

ただし，$D(\rho\|\sigma):=\operatorname{Tr}[\rho(\log\rho-\log\sigma)]$ は量子相対エントロピーで，$I(p)$ は Holevo 量子相互情報量とよばれる．独立同一拡大のケースにおいては $I(p)\ge C_r$ が示されている．不等式 $I_{BS}(p)\ge I(p)$ が示されているため [15]，(11) はタイトな評価ではないことが分かる．

各 ρ_x^n が σ_n と可換な場合，明らかに $\underline{I}(\boldsymbol{p},\boldsymbol{F})=\underline{I}_{BS}(\boldsymbol{p},\boldsymbol{F})$, $\overline{I}(\boldsymbol{p},\boldsymbol{F})=\overline{I}_{BS}(\boldsymbol{p},\boldsymbol{F})$ が成立する．より自明な場合として，ρ_{x^n} がすべて互いに可換な場合は古典的な通信路である．古典的な場合の独立同一拡大 (4) において，(12) (13) は大数の法則の直接の帰結である．このように，(7)〜(10) の情報量の性質を個別のケースで調べることは，大数の法則，中心極限

定理，大偏差原理などの純粋に (量子) 確率論的な問題である．情報スペクトル的方法では，(7)〜(10) のように極めて一般的な形の情報量を用いて符号化定理を与えることで，(量子) 情報理論特有の符号化問題と (量子) 確率論的な問題が分離されることに意義がある．上記定理の証明は以下で与えられる．

proof: Shannon のランダムコーディングと呼ばれる論法を用いる．各 $x_l^n \in \mathcal{X}^n$ $(l = 1,2,\dots,L_n)$ が，それぞれ独立に確率 p^n に従うとして，その平均について，

$$\lim_{n\to\infty} \boldsymbol{E} \left\| \frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n} - \sigma_n \right\|_1 = 0 \tag{14}$$

が示せたとするならば，少くともある系列 $\{x_1^n,\dots,x_{L_n}^n\} \subset \mathcal{X}^n$ $(n = 1,2,\dots)$ が存在して (6) を満たす．そこで，$R > \overline{I}_{BS}(\boldsymbol{p},\boldsymbol{F})$，$L_n = \lfloor e^{nR} \rfloor$ とするとき，(5) は明らかであるから，(14) を示せばよい．

各 $x^n \in \mathcal{X}^n$ について，$q_{x^n} \in \mathcal{L}(\mathcal{H}^n)$ を射影子とし，$q_{x^n}^{\perp} = 1_{\mathcal{H}^n} - q_{x^n}$，$\tau_n = E_{p^n}[\rho_{x^n}^{1/2} q_{x^n} \rho_{x^n}^{1/2}]$ とおく．このとき以下の評価が成り立つ．

$$\begin{aligned}
&\left\| \frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n} - \sigma_n \right\|_1 \\
&= \left\| \frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n}^{1/2} q_{x_l^n} \rho_{x_l^n}^{1/2} - \tau_n + \frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n}^{1/2} q_{x_l^n}^{\perp} \rho_{x_l^n}^{1/2} + \tau_n - \sigma_n \right\|_1 \\
&\le \left\| \frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n}^{1/2} q_{x_l^n} \rho_{x_l^n}^{1/2} - \tau_n \right\|_1 + \left\| \frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n}^{1/2} q_{x_l^n}^{\perp} \rho_{x_l^n}^{1/2} \right\|_1 + \left\| E_{p^n} \rho_{x^n}^{1/2} q_{x^n}^{\perp} \rho_{x^n}^{1/2} \right\|_1 \\
&\le \left\| \frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n}^{1/2} q_{x_l^n} \rho_{x_l^n}^{1/2} - \tau_n \right\|_1 + \frac{1}{L_n} \sum_{l=1}^{L_n} \left\| \rho_{x_l^n}^{1/2} q_{x_l^n}^{\perp} \rho_{x_l^n}^{1/2} \right\|_1 + E_{p^n} \left\| \rho_{x^n}^{1/2} q_{x^n}^{\perp} \rho_{x^n}^{1/2} \right\|_1
\end{aligned}$$

よってランダムコーディングについての平均をとると，

$$\boldsymbol{E} \left\| \frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n} - \sigma_n \right\|_1 \le \boldsymbol{E} \left\| \frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n}^{1/2} q_{x_l^n} \rho_{x_l^n}^{1/2} - \tau_n \right\|_1 + 2 E_{p^n} \left\| \rho_{x^n}^{1/2} q_{x^n}^{\perp} \rho_{x^n}^{1/2} \right\|_1$$

が成り立つ．この式の第二項について，Schwartz の不等式を用いると次の評価が成り立つ．

$$E_{p^n} \left\| \rho_{x^n}^{1/2} q_{x^n}^{\perp} \rho_{x^n}^{1/2} \right\|_1 \le E_{p^n} \left\| \rho_{x^n}^{1/2} \right\|_2^{1/2} \left\| q_{x^n}^{\perp} \rho_{x^n}^{1/2} \right\|_2^{1/2} \le E_{p^n} (\mathrm{Tr}[\rho_{x^n} q_{x^n}^{\perp}])^{1/2} \le (E_{p^n} \mathrm{Tr}[\rho_{x^n} q_{x^n}^{\perp}])^{1/2}$$

よって，

$$\boldsymbol{E} \left\| \frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n} - \sigma_n \right\|_1 \le \boldsymbol{E} \left\| \frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n}^{1/2} q_{x_l^n} \rho_{x_l^n}^{1/2} - \tau_n \right\|_1 + 2 (E_{p^n} \mathrm{Tr}[\rho_{x^n} q_{x^n}^{\perp}])^{1/2} \tag{15}$$

ここで $R > a > \overline{I}_{BS}(p)$ を満たす a を用いて，

$$q_{x^n} = 1_{\mathcal{H}^n} - \left\{ \rho_{x^n}^{1/2} \sigma_n^{-1} \rho_{x^n}^{1/2} > e^{na} \right\} = \left\{ \rho_{x^n}^{1/2} \sigma_n^{-1} \rho_{x^n}^{1/2} \le e^{na} \right\} \tag{16}$$

とおく．このとき $\overline{I}_{BS}(p)$ の定義 (10) と $a > \overline{I}_{BS}(p)$ により，

$$\lim_{n\to\infty} E_{p^n} \mathrm{Tr}[\rho_{x^n} q_{x^n}^{\perp}] = \lim_{n\to\infty} E_{p^n} \mathrm{Tr} \left[\rho_{x^n} \left\{ \rho_{x^n}^{1/2} \sigma_n^{-1} \rho_{x^n}^{1/2} > e^{na} \right\} \right] = 0$$

となる．したがって，(15) の第二項は $n \to \infty$ のとき 0 に収束する．

一方 (15) の第一項について，Schwartz の不等式を用いると以下の評価が成り立つ．

$$\begin{aligned}
\boldsymbol{E} \left\| \frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n}^{1/2} q_{x_l^n} \rho_{x_l^n}^{1/2} - \tau_n \right\|_1 &= \boldsymbol{E} \left\| \sigma_n^{1/2} \sigma_n^{-1/2} \left(\frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n}^{1/2} q_{x_l^n} \rho_{x_l^n}^{1/2} - \tau_n \right) \right\|_1 \\
&\le \boldsymbol{E} \left(\mathrm{Tr} \left[\sigma_n^{-1} \left(\frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n}^{1/2} q_{x_l^n} \rho_{x_l^n}^{1/2} - \tau_n \right)^2 \right] \right)^{1/2} \\
&\le \left(\boldsymbol{E} \mathrm{Tr} \left[\sigma_n^{-1} \left(\frac{1}{L_n} \sum_{l=1}^{L_n} \rho_{x_l^n}^{1/2} q_{x_l^n} \rho_{x_l^n}^{1/2} - \tau_n \right)^2 \right] \right)^{1/2} \\
&\le \left(\frac{1}{L_n} E_{p^n} \mathrm{Tr} \left[\sigma_n^{-1} \left(\rho_{x^n}^{1/2} q_{x^n} \rho_{x^n}^{1/2} - \tau_n \right)^2 \right] \right)^{1/2}
\end{aligned} \tag{17}$$

ただし最後の不等式で，$k,l=1,2,\ldots,L_n$ について

$$\boldsymbol{E}\left[\left(\rho_{x_k^n}^{1/2}q_{x_k^n}\rho_{x_k^n}^{1/2}-\tau_n\right)\left(\rho_{x_l^n}^{1/2}q_{x_l^n}\rho_{x_l^n}^{1/2}-\tau_n\right)\right]=\delta_{k,l}E_{p^n}\left[\left(\rho_{x^n}^{1/2}q_{x^n}\rho_{x^n}^{1/2}-\tau_n\right)^2\right]$$

が成り立つことを用いた．さらに，(17) の右辺について以下の評価が成り立つ．

$$\begin{aligned}\frac{1}{L_n}E_{p^n}\,\mathrm{Tr}\left[\sigma_n^{-1}\left(\rho_{x^n}^{1/2}q_{x^n}\rho_{x^n}^{1/2}-\tau_n\right)^2\right]&=\frac{1}{L_n}E_{p^n}\,\mathrm{Tr}\left[\sigma_n^{-1}\left(\left(\rho_{x^n}^{1/2}q_{x^n}\rho_{x^n}^{1/2}\right)^2-\tau_n^2\right)\right]\\&\le\frac{1}{L_n}E_{p^n}\,\mathrm{Tr}\left[\sigma_n^{-1}\left(\rho_{x^n}^{1/2}q_{x^n}\rho_{x^n}^{1/2}\right)^2\right]\\&=\frac{1}{L_n}E_{p^n}\,\mathrm{Tr}\left[\rho_{x^n}q_{x^n}\rho_{x^n}^{1/2}\sigma_n^{-1}\rho_{x^n}^{1/2}q_{x^n}\right]\\&\le\frac{e^{na}}{L_n}\end{aligned}$$

ただし最後の不等式で q_{x^n} の定義 (16) を用いた．$L_n=\lfloor e^{nR}\rfloor$ と $R>a$ より，右辺は $n\to\infty$ のとき 0 に収束する．以上で (14) が示された． □

5 量子状態伝送容量の一般公式

この節では，前節の結果から導かれる，量子状態伝送容量の一般公式について議論をする．2 節の問題設定を情報スペクトル的設定で一般化する．各 $n=1,2,\ldots$ に対して有限次元 Hilbert 空間 $\mathcal{H}_A^n$ から $\mathcal{H}_B^n$ への量子通信路 $\mathcal{E}^n:\mathcal{L}(\mathcal{H}_A^n)\to\mathcal{L}(\mathcal{H}_B^n)$ が与えられているとし，量子通信路の列を $\boldsymbol{\mathcal{E}}=\{\mathcal{E}^n\}_{n=1}^\infty$ と書く．このとき 2 節と全く同様に，“漸近的に忠実に” 伝送可能な Hilbert 空間上の量子状態全体を考え，“漸近的な符号化レート” の上限として，量子状態伝送容量 $C_q(\boldsymbol{\mathcal{E}})$ を定義することができる．この $C_q(\boldsymbol{\mathcal{E}})$ が (7)〜(10) の情報量で評価されることを示す．そのためには，メッセージ伝送量子通信路符号化定理と量子通信路 resolvability の結果が必要となる．

メッセージ伝送量子通信路符号化定理について述べる．量子通信路の列 $\boldsymbol{\mathcal{E}}=\{\mathcal{E}^n\}_{n=1}^\infty$ を用いて，古典的メッセージの増大列 $\{1,2,\ldots,M_n\}$ $(n=1,2,\ldots)$ を伝送することを考える．メッセージに応じて異る量子状態を伝送し，受信側では量子力学的測定により元のメッセージを推定してやるのである．このとき “漸近的に誤りなく” 伝送可能なメッセージの “漸近的な符号化レート” $\liminf_{n\to\infty}\frac{1}{n}\log M_n$ の上限として，メッセージ伝送通信路容量 $C_{cq}(\boldsymbol{\mathcal{E}})$ が定義される．このとき次の定理が成り立つ．

Proposition 2 (Hayashi-Nagaoka [18])

$$C_{cq}(\boldsymbol{\mathcal{E}})=\sup_{\boldsymbol{p}}\underline{I}(\boldsymbol{p},\boldsymbol{\mathcal{E}}) \tag{18}$$

ただし，sup は $\mathcal{S}(\mathcal{H}_A^n)$ 上の確率測度 p^n の列 $\boldsymbol{p}=\{p^n\}_{n=1}^\infty$ についてとり，$\underline{I}(\boldsymbol{p},\boldsymbol{\mathcal{E}})$ は (7) で定義される情報量である．(より詳しくは，$\underline{I}(\boldsymbol{p},\boldsymbol{\mathcal{E}})$ が “achievable” であることが証明されている．)

ここで各 $n=1,2,\ldots$ について，量子通信路 $\mathcal{E}^n$ の Stinespring-Kraus 表現を与える Hilbert 空間を $\mathcal{H}_E^n$，等距離作用素を $V_n:\mathcal{H}_A^n\to\mathcal{H}_B^n\otimes\mathcal{H}_E^n$ とする．すなわち，$\mathcal{E}^n(\rho)=\mathrm{Tr}_{\mathcal{H}_E^n}[V_n\rho V_n^*]$ とする．また，量子通信路 $\mathcal{F}^n:\mathcal{L}(\mathcal{H}_A^n)\to\mathcal{L}(\mathcal{H}_E^n)$ を $\mathcal{F}^n(\rho)=\mathrm{Tr}_{\mathcal{H}_B^n}[V_n\rho V_n^*]$ で定義し，これら量子通信路の列を $\boldsymbol{\mathcal{F}}=\{\mathcal{F}^n\}_{n=1}^\infty$ とおく．このとき，Devetak の論法 [4] により，上記の Proposition 2 と前節の結果を用いることで，量子状態伝送容量 $C_q(\boldsymbol{\mathcal{E}})$ は次式で評価される．

Theorem 3

$$C_q(\mathcal{E}) \geq \sup_{\boldsymbol{p}} [\underline{I}(\boldsymbol{p},\mathcal{E}) - C_r(\boldsymbol{p},\mathcal{F})]$$
$$\geq \sup_{\boldsymbol{p}} [\underline{I}(\boldsymbol{p},\mathcal{E}) - \overline{I}_{BS}(\boldsymbol{p},\mathcal{F})] \quad (19)$$

ただし，sup は $\mathcal{S}(\mathcal{H}_A^n)$ 上の確率測度 p^n の列 $\boldsymbol{p} = \{p^n\}_{n=1}^{\infty}$ についてとり，$\underline{I}(\boldsymbol{p},\mathcal{E})$, $\overline{I}_{BS}(\boldsymbol{p},\mathcal{F})$ は (7) (10) で定義される情報量である．

参考文献

[1] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, no. 5, pp. 793–797, 1996.

[2] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, no. 4, pp. R2493–R2496, 1995.

[3] P. W. Shor, "The quantum channel capacity and coherent information." Lecture Notes, MSRI Workshop on Quantum Computation, 2002.

[4] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. Inform. Theory*, vol. 51, no. 1, pp. 44–55, 2005.

[5] M. Hayashi, *Quantum Information Theory: An Introduction.* Berlin: Springer, 2006. (林正人, 量子情報理論入門, サイエンス社, 2004).

[6] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Phys. Rev. Lett.*, vol. 83, no. 3, pp. 648–651, 1999.

[7] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, "Quantum secret sharing schemes and reversibility of quantum operations," *Phys. Rev. A*, vol. 72, 032318, 2005.

[8] T. S. Han, *Information Spectrum Methods in Information Theory.* Berlin: Springer, 2003. (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).

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information.* Cambridge: Cambridge University Press, 2000.

[10] B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction," *Phys. Rev. A*, vol. 54, no. 4, pp. 2629–2635, 1996.

[11] H. Barnum, E. Knill, and M. A. Nielsen, "On quantum fidelities and channel capacities," *IEEE Trans. Inform. Theory*, vol. 46, no. 4, pp. 1317–1329, 2000.

[12] E. Knill and R. Laflamme, "Theory of quantum error-correcting codes," *Phys. Rev. A*, vol. 55, no. 2, pp. 900–911, 1997.

[13] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, no. 5, pp. 3824–3851, 1996.

[14] Y. Ogata, "Decoherence-free algebra," *Physics Letters A*, vol. 314, no. 1-2, pp. 19–22, 2003.

[15] F. Hiai and D. Petz, "The proper formula for relative entropy and its asymptotics in quantum probability," *Commun. Math. Phys.*, vol. 143, pp. 99–114, 1991.

[16] T. Ogawa and H. Nagaoka, "Strong converse and Stein's lemma in quantum hypothesis testing," *IEEE Trans. Inform. Theory*, vol. 46, no. 7, pp. 2428–2433, 2000.

[17] H. Nagaoka and M. Hayashi, "An information-spectrum approach to classical and quantum hypothesis testing for simple hypotheses," e-print quant-ph/0206185, 2002.

[18] M. Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels," *IEEE Trans. Inform. Theory*, vol. 49, no. 7, pp. 1753–1768, 2003.